Critical infrastructure protection by advanced modelling, simulation and optimization for cascading failure mitigation and resilience

Yiping Fang

ÉCOLE CENTRALE DES ARTS
ET MANUFACTURES
« ÉCOLE CENTRALE PARIS »

THÈSE

présentée par

Yiping FANG

pour l'obtention du

GRADE DE DOCTEUR

Spécialité : Genie Industriel

Laboratoire d'accueil : Laboratoire de Genie Industriel

SUJET :

Critical Infrastructure Protection by Advanced Modelling, Simulation and Optimization for Cascading Failure Mitigation and Resilience

Protection des Infrastructures Essentielles par Advanced Modélisation, Simulation et Optimisation pour l'Atténuation et Résilience de Défaillance en Cascade

soutenue le : 2 Fevrier 2015

devant un jury composé de :

Giovanni Sansavini	ETH Zürich	Reviewer
Roberto Setola	Università Campus Bio-Medico	Reviewer
Stéphane Andrieux	Électricité de France R&D	Examiner
Georgios Giannopoulos	Joint Research Centre European Commission	Examiner
Enrico Zio	École Centrale Paris	Supervisor

2015ECAP0013

Acknowledgements

First of all, I would like give my sincere appreciation to my thesis advisor, Professor Enrico Zio, for picking me as his PhD student; thank him for picking this day for my Phd defense, because it was exactly the same day three years ago that I arrived at France; thank him for pushing me when I want (I mean, when I really don't want to work); thank him for deciding to exempt my additional ten years Phd study – my punishment of losing so many chances to score as his football teammate; and thank him, seriously, for being my career role model with his strong enthusiasm and passion for the scientific research and his rigorous organization of the work.

I want to thank Dr. Nicola Pedroni, my co-advisor, for his presence at my PhD defense, because I was supposed to buy him a beautiful blue dress in compensation for my mistaking him as my "Co-directrice" (the feminine of the word "co-advisor" in French); but I didn't. Seriously, he is a wonderful person. Thank him for his advice, patience and great support during my PhD study. It is my great pleasure to work with him!

My deepest appreciation goes to all the jury members, Professor Giovanni Sansavini, Professor Roberto Setola, Dr. Stéphane Andrieux and Dr. Georgios Giannopoulos, who agreed to be part of the committee. I am very pleased to have presented my Ph. D. work in front of such high qualified jury. Special thanks to the reviewers, Professor Giovanni Sansavini and Professor Roberto Setola, for the evaluation of the manuscript and all the constructive and helpful remarks.

Besides, I would like to thank Dr. Yanfu Li, for his kindness and help. It's so lucky to have a so kind Chinese professor in the group, that I would not feel I had been kidnapped by the "Italian Mafia". I want to thank every chair member: Elisaveta, Ronay, Rodrigo, Jie, Lo, Tairan, Elisa, Xing, Yanhui, Fangyuan, Ionela, Carlos, and Valeria. I am so lucky to work with these wonderful persons! They are so awesome; even some of them have graduated before me. Besides, I would like to give my special thanks to my officemate, dear Elisa and Tairan. It is a funny, fruitful and unforgettable memory to work with them together in the same office for three years.

I would like to thank all of my colleagues from Industrial Engineering Laboratory (LGI). It's my great pleasure to be working here, to be one of the members in this laboratory! We have so many precious memories as a unit, such as the "Labo Cup", Séminaire.

I would like to acknowledge Professor Jean-Claude Bocquet, Director of the laboratory. I still remember his welcome speech in the first day that I arrived here; it was so warm, and so wonderful, just one problem: I couldn't understand any single word he said, except "Bienvenue"! My warmest recognition goes to Corinne Ollivier, Delphine Martin and Sylvie Guillemain, the secretaries of LGI, because they have been lovely in helping me to overcome the initial difficulties of integration in France and their kind work has eased mine.

From the bottom of my heart, thank to my dear girlfriend, Jingjiao, for accompanying me, understanding me, sharing with me.

Finally, I wish to dedicate this thesis to my family, my parents and my little brother who have always been there for me with a truthful support.

Abstract

Continuously increasing complexity and interconnectedness of modern critical infrastructures, together with increasingly complex risk environments, pose unique challenges for their secure, reliable, and efficient operation. The focus of the present dissertation is on the modelling, simulation and optimization of critical infrastructures (CIs) (e.g., power transmission networks) with respect to their vulnerability and resilience to cascading failures. This study approaches the problem by firstly modelling CIs at a fundamental level, by focusing on network topology and physical flow patterns within the CIs. A hierarchical network modelling technique is introduced for the management of system complexity. Within these modelling frameworks, advanced optimization techniques (e.g., non-dominated sorting binary differential evolution (NSBDE) algorithm) are utilized to maximize both the robustness and resilience (recovery capacity) of CIs against cascading failures. Specifically, the first problem is taken from a holistic system design perspective, i.e. some system properties, such as its topology and link capacities, are redesigned in an optimal way in order to enhance system's capacity of resisting to systemic failures. Both topological and physical cascading failure models are applied and their corresponding results are compared. With respect to the second problem, a novel framework is proposed for optimally selecting proper recovery actions in order to maximize the capacity of the CI network of recovery from a disruptive event. A heuristic, computationally cheap optimization algorithm is proposed for the solution of the problem, by integrating foundemental concepts from network flows and project scheduling. Examples of analysis are carried out by referring to several realistic CI systems.

Key words: critical infrastructure protection, complex network, cascading failure, system modelling, simulation, optimization

Résumé

Sans cesse croissante complexité et l'interdépendance des infrastructures critiques modernes, avec des environs de risque plus en plus complexes, posent des défis uniques pour leur exploitation sûre, fiable et efficace. L'objectif de la présente thèse est sur la modélisation, la simulation et l'optimisation des infrastructures critiques (par exemple, les réseaux de transmission de puissance) à l'égard de leur vulnérabilité et la résilience aux défaillances en cascade. Cette étude aborde le problème en modélisant infrastructures critiques à un niveau fondamental, en se concentrant sur la topologie du réseau et des modèles de flux physiques dans les infrastructures critiques. Un cadre de modélisation hiérarchique est introduit pour la gestion de la complexité du système. Au sein de ces cadres de modélisation, les techniques d'optimisation avancées (par exemple, non-dominée de tri binaire évolution différentielle (NSBDE) algorithme) sont utilisés pour maximiser à la fois la robustesse et la résilience (capacité de récupération) des infrastructures critiques contre les défaillances en cascade. Plus précisément, le premier problème est pris à partir d'un point de vue de la conception du système holistique, c'est-à-dire certaines propriétés du système, tels que ses capacités de topologie et de liaison, sont redessiné de manière optimale afin d'améliorer la capacité de résister à des défaillances systémiques de système. Les deux modèles de défaillance en cascade topologiques et physiques sont appliquées et leurs résultats correspondants sont comparés. En ce qui concerne le deuxième problème, un nouveau cadre est proposé pour la sélection optimale des mesures appropriées de récupération afin de maximiser la capacité du réseau d'infrastructure critique de récupération à partir d'un événement perturbateur. Un algorithme d'optimisation de calcul pas cher heuristique est proposé pour la solution du problème, en intégrant des concepts fondamentaux de flux de réseau et le calendrier du projet. Exemples d'analyse sont effectués en se référant à plusieurs systèmes de CI réalistes.

Mots clés: protection des infrastructures critiques, réseau complexe, l'échec en cascade, la modélisation du système, simulation, optimisation

Contents

List of Figures

List of Tables

Acronyms

AC	Alternating Current
BI	Birnbaum Importance
CDF	Cumulative Distribution Function
CI	Critical Infrastructure
CIM	Critical Importance Measure
CIP	Critical Infrastructure Protection
CM	Copeland Method
CML	Coupled Map Lattice
DC	Direct Current
EBI	Extended Birnbaum Importance
ECI	Extended Crticality Importance
EFVI	Extended Fuessell & Vesely Importance
FKM	Fuzzy k-means
FPTN400	The 400kV French Power Transmission Network
IPTN380	The 380kV Italian Power Transmission Network
ML	Motter & Lai Cascading Failure Model
MOEA	Multi-Objective Evolutionary Algorithm
MODE	Multi-Objective Differential Evolution
NSBDE	Non-donminated Sorting Binary Differential Evolution
NSGA-II	Non Dominated Sorting Genetic Algorithm II
OPA	ORNL-PSerc-Alaska Cascading Failure Model
ORT	Optimal Repair Time
ROP	Resilience Optimization Problem
SOC	Self-Organized Criticality
TPR	Terminal Pair Reliabitliy
USCA	Unsupervised Spectral Clustering Algorithm
WSPT	Weighed Shortest Processing Time

Appended papers

Paper [1] Y.-P. Fang, E. Zio. “Unsupervised spectral clustering for hierarchical modelling and criticality analysis of complex networks.” Reliability Engineering and System Safety, 116:64-74, 2013.

Paper [2] Y.-P. Fang, E. Zio. “Hierarchical Modelling by Recursive Unsupervised Spectral Clustering and Network Extended Importance Measures to Analyze the Reliability Characteristics of Complex Network Systems.” American Journal of Operation Research, 3(1A): 101-112, 2013.

Paper [3] Y.-P. Fang, N. Pedroni, E. Zio. “Network-centric Optimization of Failure Resilient Electrical Infrastructures and its Validation by Power Flow Model.” Risk Analysis, Accepted, 2014.

Paper [4] Y.-P. Fang, N. Pedroni, E. Zio. “Comparing network-centric and power flow models for the optimal allocation of link capacities in a cascade-resilient power transmission network.” IEEE System Journal, vol.PP, no.99, pp.1,12, 2014.

Paper [5] Y.-P. Fang, N. Pedroni, E. Zio. “Assessment and optimization of system resilience for infrastructure network systems.” IEEE System Journal, 2014, under review.

Paper [6] Y.-P. Fang, N. Pedroni, E. Zio. “Resilience-based component importance measures for infrastructure network systems.” Reliability, IEEE Transaction on, 2014, under review.

Chapter 1 Introduction

World-wide social and economic stability is becoming increasingly dependent on reliable supply of essential goods and services, that are transported and distributed across large technological networked infrastructure systems, also called critical infrastructures (CIs). These goods and services (e.g. electrical power, gas and water, transportation, telecommunication, etc.) are largely taken for granted, their production and delivery being assumed to never cease. On the other hand, the infrastructure systems that allow their supply are challenged by potential disruptive factors coming from the risky environments they are operated in: global warming, disease outbreaks, food (distribution) shortages, financial crashes, heavy solar storms, organized (cyber-) crime, or cyber warfare. Also, the infrastructure networks have been growing independently and very fast, in a somewhat uncontrollable manner, creating underlying pathways along which dangerous hazards and damaging events can spread rapidly and globally throughout the system: this has increased the exposure to systemic risk, characterized by cascades of failures which can have significant impacts at the global system scale (Helbing, 2013).

Indeed, large-scale disruptions have been experienced, confirming the existence of inherent vulnerabilities. On 28 September 2003, there was a serious power outage that affected much of Italy for 12 hours and part of Switzerland for 3 hours, affecting a total of 56 million people and resulting in tens of millions of dollars in economic losses (U.C.T.E, 2004). In the same year, another power blackout happened in North America, affecting 50 million people and causing estimated losses for $10 billion U.S. dollars (U.S.-CA, 2004). Other incidents like these, where technical infrastructures failed and led to major disruptions, include the ice-storm in Canada in 1998 (Chang et al., 2007), the power outage that affected half of Europe in 2006 due to the crash of the luxury line Norwegian Pearl ship onto a power line (U.C.T.E, 2006) and the hurricane Katrina in 2007, which wiped out most of the CIs in the New Orleans area for a considerable amount of time, severely crippling recovery operations (Boin and McConnell, 2007).

Many questions stem from the occurrence of these extreme incidents involving CIs: What is the inherent vulnerability of a CI system and which are its critical components that if they fail cause large consequences? What is the mechanism of the propagation of failures in the CI system? How will the CI system react to unexpected events and how large can the consequences become? Are there particular properties that allow the CI to resist to systemic failures? How to define the resilience of the CI system? How to find an 'optimal' strategy for the system to recover from disruption? The motivation behind this thesis is to address the type of quesitons stated above; the objective of the thesis is to study and develop advanced modelling, simulation, analysis and optimization methods for the protection of CIs against systemic failures.

This chapter aims to provide a general overview of the problems addressed in this dissertation, and is organized as follows. CIs are defined and their characteristics are introduced in Section 1.1; in Section 1.2, the key concepts of risk, vulnerability and resilience of CIs are discussed; Section 1.3 specifies the objectives of the research conducted; finally, in Section 1.4, the structure of the dissertation is given.

1.1 CI systems as complex engineering networks

The phrase, "critical infrastructure protection (CIP)," did not appear in print until in 1997, when the "Marsh report" (Ellis, 1997) provided the first definition of infrastructure as

> *"a network of independent, mostly privately-owned, man-made system that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services".*

Critical infrastructures (CIs) are defined as network systems that provide life-essential services (McCarthy et al., 2005) and their incapacity or destruction would have a debilitating impact on the health, safety, security, economics, and social well-being, including the effective functioning of governments (Kröger and Zio, 2011). CIs are various by nature, e.g., physical-engineered, cybernetic or organizational systems, and by environment (geographical, natural) and operational context (political, economic, etc.).

The focus of this thesis is on engineered physically networked CIs, often called *lifeline* systems; examples of these networks are those providing (Kröger and Zio, 2011):

- Energy (electricity, oil, and gas supply)
- Transportation (by rail, road, air, and sea)
- Information and telecommunication (such as the Internet)
- Computer networks such as the Internet
- State and local services (water supply and emergency services).

From a European Union perspective, a programme on Prevention, Preparedness and Consequence Management of Terrorism and Other Security Related Risks (EPCIP) was adopted on 12 February 2007. In the act (COM, 2006, p. 15) CIs are defined as "…those assets or parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economic or social well-being of people". In particular, electrical power supply stands out as an especially critical infrastructure since many other infrastructures depend heavily on a reliable power supply.

Engineered CI systems, usually distributed on large geographical extensions, are complex collections of a large number of interacting elements (or subsystems) having an internal dynamic structure and comprising a unified whole. They present several common characteristics that make them difficult to control or to operate reliably and efficiently (Amin, 2001):

- They have a large-scale, multi-component, heterogeneous and distributed nature;
- They are vulnerable to attacks and local disturbances which can lead to widespread cascading failure almost instantaneously;
- They are characterized by many points of interaction among a variety of participants – owners, operators, sellers, buyers, customers, data and information providers, data and information users;
- The number of possible interactions increases dramatically as participants are added; thus, no single centralized entity can evaluate, monitor, and manage all the interactions in real time;
- The conventional mathematical methodologies that underpin today's modeling, simulation, and control paradigms are unable to handle their complexity and interconnectedness.

As Zio (2007) and Kröger (2008) point out, in order to address the complexities of CI systems new methods for their analysis are needed, since "…the current quantitative methods of risk analysis seem not to be fully equipped to deal with the level of complexity inherent in such systems" (Zio, 2007, p. 505).

1.2 Risk, vulnerability and resilience of CIs

1.2.1 Risk and systemic risk

While the concept of risk is fairly mature and consensually agreed, the concepts of vulnerability and resilience are still evolving and not yet established. One definition of risk often used in system engineering is that it is "a function of the probability of an unwanted event and the severity of consequences of that event" (Kaplan and Garrick, 1981):

$$Risk = \{\langle S_i, L_i, X_i \rangle\} \tag{1.1}$$

where S_i denotes the ith risk scenario, L_i denotes the likelihood of that scenario, and X_i denotes the resulting consequences.

These quantities and their associated uncertainties are considered as being numerically quantifiable: e.g., for CIs, risk can be computed as the loss of service with its resulting consequences for the people concerned. Today's infrastructure networks are challenged by the disruptive influences of a complex mix of manmade and naturally occurring threats and hazards, including terrorist attacks, accidents, natural disasters, and other emergencies.

Systemic risk is the risk of having not just statistically independent failures, but interdependent, *cascading failures* in a network of N interconnected system components (Helbing, 2013). In other words, systemic risk results from connections between risks ('networked risks'), whereby a localized initial failure ('perturbation') could spread to other parts of the system and have system-scale disastrous effects. Then, the examples of system-scale damages mentioned before on real-world CI systems confirm the existence of systemic risks: blackouts in power grids (U.S.-CA, 2004; U.C.T.E, 2004; 2007; Pidd, 2012), telecommunication outages (Newman et al., 2002), financial bankruptcy (Battiston et al., 2007), and catastrophic failures in socio-economic systems (Zhao et al., 2011; Kempe et al., 2003). Figure 1:1 shows the historical frequency of large electrical blackouts happened in the North American Power Grid: an increasing trend of occurrence of large blackouts can be observed.

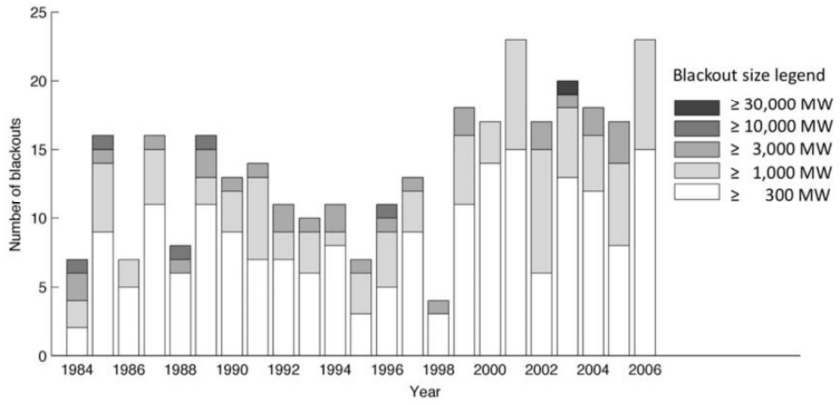


Figure 1:1 Number of large blackouts per year happened in North America after removing small events, adjusting for demand growth, and removing extreme natural events (Hines et al., 2009).

Although large-scale disruptions are rare if compared with small ones, how much rarer are they? If the frequency of incidents, both natural and manmade, is plotted against the consequences, the trend is a power law (rather than exponential) distribution (e.g. Amin, 2004; Nedic et al., 2006; Weron and Simonsen, 2006, as shown in Figure 1:2). Then, if we were to evaluate the risk of a disruption as the product of frequency times consequence, the total risk associated with large-scale disruptions is – due to the power-law type distribution of blackout sizes – much larger than that associated to small failures. This is strong motivation for investigating the global dynamics of systemic risks that can lead to power-law tails.

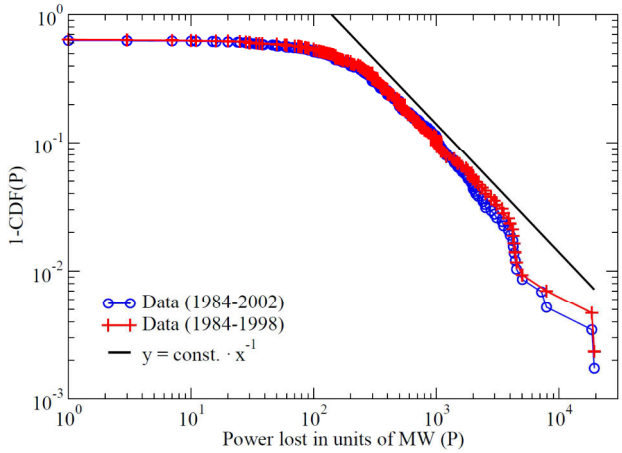


Figure 1:2 The complimentary cumulative distribution $(1 - CDF(P))$ of power lost (P) due to blackouts in the North-American electric power transmission systems (Weron and Simonsen, 2006).

1.2.2 Vulnerability

Vulnerability is a concept that is used in many areas, but its definition is often ambiguous and sometimes misleading (Buckle et al., 2000; Dilley and Boudreau, 2001; Weichselgartner, 2001; Haimes, 2006). Many definitions look at vulnerability as the system's overall susceptibility to loss due to a given negative event. In order for the vulnerability definition to be meaningful, it must be related to specific hazard exposures (e.g. Dilley and Boudreau, 2001). A system might, thus, be vulnerable to certain hazard exposures but robust and resilient to others (Hansson and Helgesson, 2003).

The vulnerability of a system can be analyzed mainly from two perspectives. The first one relates to a global system property, whereby one looks at the extent of adverse effects caused by the occurrence of a specific hazardous event (e.g., Aven, 2007; Johansson and Hassel, 2010; Kröger and Zio, 2011). The second perspective looks at the critical parts or components of the system, which make it vulnerable (e.g., Apostolakis and Lemon, 2005; Latora and Marchiori, 2005).

In this dissertation, we espouse the concept of vulnerability as a measure of "*the consequences that arise when a system is exposed to a hazardous event of a given type and magnitude*" and we adopt both perspectives of vulnerability analysis mentioned above: specifically, in appended Paper [1], the term "vulnerability analysis" refers to the identification of critical components of CIs, whereas in appended Papers [3] and [4], "vulnerability" is related to the global property of the CI system, which is quantified by the extent of adverse effects caused by the occurrence of a specific disruptive event.

1.2.3 Resilience

Resilience comes from the Latin word "resilio" that literary means "to leap back" and denotes a system attribute that characterizes the ability to recover from challenges or disruptive events. The Merriam-Webster dictionary defines resilience as "the ability to recover from or adjust easily to misfortune or change". Various definitions of "resilience" have been proposed for infrastructure and economic system analysis in the past decades (e.g., Holling, 1973; Bruneau et al., 2003; Reed et al., 2009; Cimellaro et al., 2010; Aven, 2011; Henry and Emmanuel Ramirez-Marquez, 2012). In general, it can be said to be the ability of a system or an organization to react and recover from unanticipated disturbances and events (e.g., Hollnagel et al., 2006). Zio (2009, p. 131) advances the view of resilience as complementing reliability by stating "… *systems should not only be made reliable, i.e. with acceptably low failure probability, but also resilient, i.e. with the ability to recover from disruptions of the nominal operating conditions*".

An integrated definition of resilience is given by McDaniels et al. (2007). This definition points out two key properties of resilience, namely *robustness* and *recovery rapidity*. *Robustness* refers to a system's ability to withstand a certain amount of stress with respect to the loss of function of the system, or as Hansson and Helgesson (2003) defines it: "*the tendency of a system to remain unchanged, or nearly unchanged, when exposed to perturbations*". In this view, *robustness* can be seen as the antonym of the term *vulnerability*. *Recovery rapidity*, on the other hand, refers to a system's ability to recover fast from an undesired event.

Currently, there is the feeling of a lack of standardization and rigor when quantitatively defining resilience (Henry and Emmanuel Ramirez-Marquez, 2012). Too many different and subjective definitions make resilience appear to be just another buzzword and not an attribute of engineering systems. To address this issue, this dissertation (Chapter 4.1) reviews some resilience metrics and measurement methodologies in the context of system engineering, especially for CI systems; then, it proposes a novel definition and quantification of system resilience, rigorously focusing on the post-disruption recovery process, which embraces both the *spatial* (functionality recovery) and *temporal* (recovery time) dimensions of resilience. The details of this definition and relevant discussion will be given in Chapter 4.1.

From a synthetic disaster management perspective, Figure 1:3 conceptually illustrates all the concepts mentioned, i.e., risk, vulnerability, robustness and resilience, and their characteristics with reference to the functionality curve $F(t)$ of a CI system, which represents the evolution of the functional state of a system (Cimellaro et al., 2010; Henry and Emmanuel Ramirez-Marquez, 2012). In the Figure, S_i denotes a risk scenario, L_i denotes the likelihood of that scenario, $\tilde{X}_i$ is a random variable denoting the resulting consequence (functionality loss) and is expressed as function of the uncertainty σ_i associated with it.

Then, the quantification of *risk* in Equation 1.1 can be rewritten as

$$Risk = \left\{ \left\langle S_i, L_i, \tilde{X}_i(\sigma_i) \right\rangle \right\} \tag{1.2}$$

Vulnerability referring to the CI system is "the consequences that arise when the system is exposed to a hazardous event of a given type and magnitude" and can be represented by the random variable $\tilde{X}_i(\sigma_i)$.

$$Vulnerability = \left\{ \left\langle \tilde{X}_i(\sigma_i) \right\rangle \right\} \tag{1.3}$$

Anther random variable $\widetilde{R}_i$ denotes the *robustness* (defined as "*the tendency of a system to remain unchanged, or nearly unchanged, when exposed to perturbations*") of the system under risk S_i. It is the residual functionality right after the disruptive event and can be represented by the following relation:

$$Robustness = \left\{ \left\langle \widetilde{R}_i \right\rangle \right\} = \left\{ \left\langle F(t_0) - \tilde{X}_i(\sigma_i) \right\rangle \right\} \tag{1.4}$$

On the post-disruption recovery process, $T_{RE}(t_r)$ denotes the time duration required for the system to achieve a target functionality level $F(t_r)$, and the restored system functionality is $F_{RE}(t_r)$. The two quantities represent the *spatial* and *temporal* dimensions of *resilience*, respectively. Therefore,

$$Resilience(t_r) = \{\langle T_{RE}(t_r), F(t_r) \rangle\} \tag{1.5}$$

One can refer to Chapter 4.1 and the appended Paper [5] for the analytic expression of Equation (1.5).

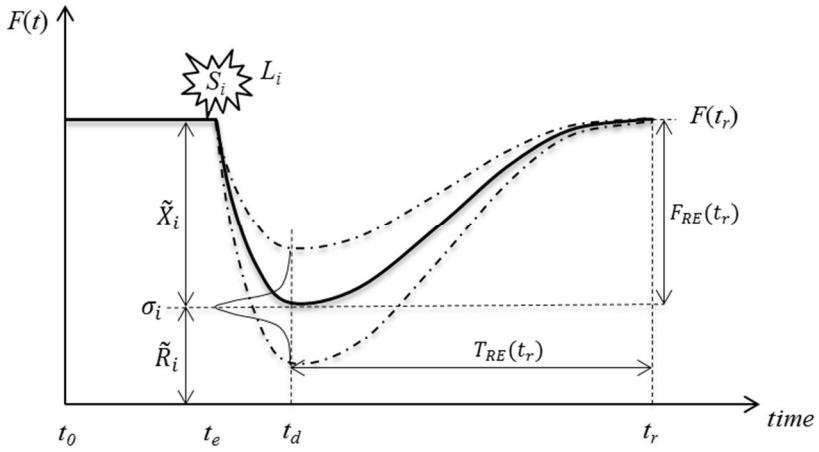


Figure 1:3 Conceptual illustration of the concept of risk, vulnerability, robustness and resilience, with reference to the functionality curve $F(t)$ of a CI system.

1.3 Research objectives

CIs can operate in three distinct functional states: 1) stable state, 2) disrupted state, and, 3) recovered state, and two transitions: 1) system disruption (from the stable state to the disrupted state), and 2) system recovery (from the disrupted state the recovered state). There are two events that trigger and enable these two transitions: a disruptive event and the resilience action. In Figure 1:4, the different states and transitions are illustrated. For the point of view of disaster management, before the occurrence of a disruptive event, actions and activities (e.g., upgrading vulnerable parts of the system, allocating preventive resources and so on) are usually taken in order to mitigate the likelihood and/or consequences of an undesired event. On the other hand, after the disruption, there is a recovery process in which resilience actions (e.g., an overall recovery planning) are taken for the system to return to a normal or desired state.

The present dissertation takes into account the entire state transition process of CIs under disruptive event, and focuses on the modelling, simulation and optimization of CI systems (e.g., power transmission networks), with respect to their *vulnerability* and *resilience* to cascading failures. The research objectives, which represent also the main contributions of this dissertation, are divided into three groups:

- Static representation and analysis of CI networks:

- To develop network models suitable for the representation of CI networks;
- To develop performance metrics for quantifying generic network functionality;
- To identify the role that various network components have in maintaining the performance of the entire network (e.g., connectivity or reliability).

- Optimal CI design for cascading failure mitigation:
  - To establish optimization frameworks for designing CI systems robust against cascading failures, with limited cost;
  - To conduct a thorough comparative study among different methodologies for the modelling of cascading failures;
  - To propose effective and efficient solution algorithms for the proposed optimization problems.
- Recovery optimization for system resilience:
  - To propose a formal, rigorous definition of the concept of system resilience;
  - To develop dynamic recovery models for post-disaster system restoration;
  - To construct a comprehensive framework for properly selecting recovery actions in order to optimize system resilience when resources are limited;
  - To design effective and efficient algorithms for solving the proposed resilience optimization problem;
  - To identify the role that various network components have in contributing to the resilience of a CI system.

In Figure 1:4, we have summarized the main research objectives of this thesis in a flow chart that shows the basic dependencies between the objectives and their organization in this dissertation.

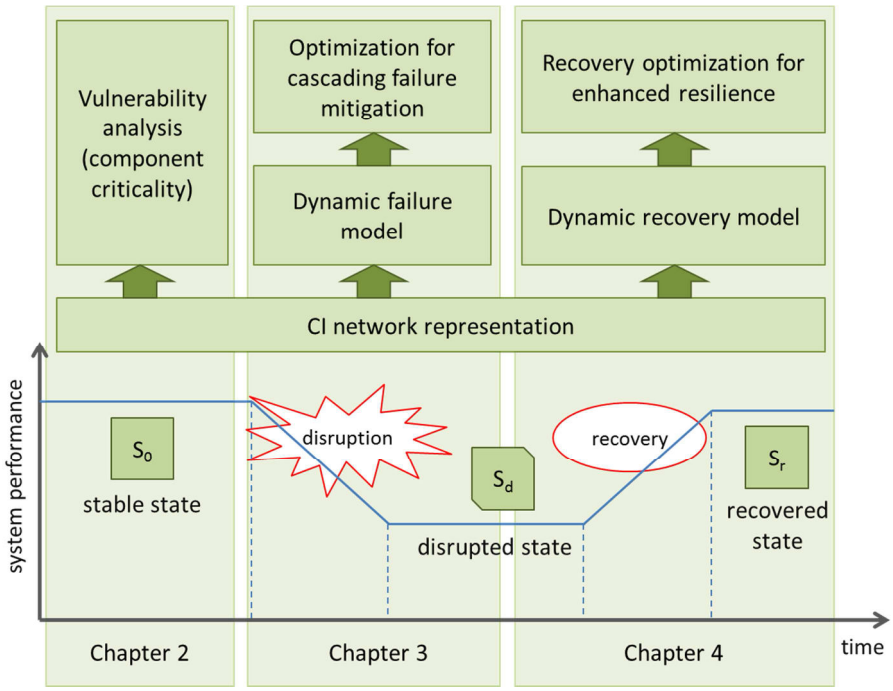


Figure 1:4 Pictorial view of the research presented in this dissertation.

1.4 Structure of the thesis

The thesis is composed of two parts. Part I, subdivided in six Chapters, introduces and addresses in details the problems treated and illustrates the methodological approaches developed and employed in this Ph. D. work. Part II is a collection of six selected papers published, submitted for publication or under submission as a result of the work, and which the reader is referred to for further details.

Chapter 2 starts with a brief critical discussion of the approaches based on complex network theory that have been employed for the analysis of CIs. Then, a general hierarchical modelling framework for representing CI networks is proposed, which can be leveraged efficiently to facilitate the management of complexity in the analysis of large-scale CI systems. Moreover, several metrics are introduced for identifying those components within the system that most significantly influence the system reliability.

In Chapter 3, two different cascading failure modelling approaches of increasing complexity, i.e. a complex network-based model and a physical flow-based model (for electrical power grids), are embraced to address the problem of redesigning network properties (e.g., topology and link capacity). This problem is formulated within a multi-objective optimization framework and solved by evolutionary algorithms.

Chapter 4 focuses on the study of system *resilience*. A quantitative definition of the concept of resilience for CI systems is given: based on this definition, an optimization framework is proposed for properly selecting recovery actions in order to maximize the resilience of a CI network. A heuristic dispatching rule is presented to timely solve the associated resilience optimization problem. Furthermore, two metrics are originally introduced to measure the criticality of network components from the perspective of their contribution to system resilience.

Chapter 5 contains the applications of the proposed models and methodologies to realistic CI networks (in particular, the 380kV Italian Power Transmission Network, the 400kV French Power Transmission Network and the IEEE 30 Bus test system). Chapter 6 draws the conclusions of this PhD study and presents relevant open issues and perspectives for future research.

Part II of this thesis includes the collection of papers published and submitted, which constitute the pillars of the present doctoral thesis. Papers [1] and [2] present the hierarchical representation framework and its application to network reliability and vulnerability analysis (see Chapter 2 and Chapter 5.1 of Part I). Papers [3] and [4] concern CI optimization against cascading failures (see Chapter 3 and Chapter 5.2). Specifically, Paper [3] addresses the problem of network topology optimization by rewiring links under the objectives of maximizing network robustness to cascading failure and minimizing investment costs. The realistic character of the optimization results based on a computationally-cheap, topological cascading failure model is verified by a more realistic power flow-based model of cascading failure. In Paper [4], for the sake of comparison, both types of models (i.e., topological and power flow-based) are embraced to address the optimization of link capacity allocation against cascading failures. Papers [5] and [6] form the basis for the study of system resilience in Chapters 4, 5.3 and 5.4. The quantitative definition of system resilience, the formulation of a resilience optimization problem and the development of a heuristic dispatching rule for its solution are the main contributions of Paper [5]. Finally, Paper [6] mainly contributes two resilience-based component importance measures.

Chapter 2 Network modelling of CI systems

The modelling of any real-life system requires well-defined system boundaries and usually simplifications of the system representation: Such boundaries and simplifications are determined by the context in which the model is used. The aim of the chapter is to critically review previous inspiring research regarding the modelling of CI systems as well as to describe the author's proposed modelling approach. In particular, the first Section briefly introduces the field of complex network theory and how CIs can be represented in the framework of network theory. The second Section develops a general hierarchical modelling framework, based on statistical clustering techniques, for representing CI networks. In the last Section, we propose several metrics for identifying those components within the system that most significantly influence system reliability.

2.1 Complex network theory and network representation of CI systems

2.1.1 Complex network theory

The ideas behind the research described in the present dissertation stem partly from the field of complex network theory. The "predecessor" of complex network theory is the mathematical field of graph theory, initiated by Leonhard Euler and the "seven Bridges of Königsberg problem" in 1736. Further advances in the field were not made until 1959, when two Hungarian mathematicians, namely, Paul Erdös and Alfred Rényi, developed the theory of *random networks*. They introduced the use of probabilistic methods to demonstrate the existence of graphs with particular properties, such as *network connectivity* (Erdös and Rényi, 1959).

Researchers and scientists did not realize that modelling real complex networks required a shift in paradigm, despite the convenience and mathematical insights provided by random graphs models, the insights from empirical studies on social networks, and the ideas for optimal design of resilient networks. This only happened in the late 1990's, when databases from several disciplines became readily available, and general features of complex networks started to be uncovered. Sociologists, mathematicians, physicists and engineers joined forces to formally develop the new science of a connected age (Watts, 2004). Two pioneering works in this field concern the findings of *small-world* (Watts and Strogatz, 1998) and *scale-free* (Barabási and Albert, 1999) networks.

The basic concept of complex network theory is to build a model of real-world networks and describe the form and, in various degrees, the functionality of the network by different measures. Complex network theory has been used to study a wide range of systems, such as: social networks (e.g. celebrity networks), technical networks (e.g. the Internet and electrical power systems), cellular networks, and the studies of the written human language (Albert and Barabási, 2002). The reader can refer to numerous works for a comprehensive review of the study in this field (e.g., Newman, 2003; Watts, 2004; Boccaletti et al., 2006; Grubesic et al. 2008).

For network theoretical studies of CIs, only the most fundamental parts of the infrastructure are usually modelled, i.e. the structural properties of the system that facilitates the physical transportation of the services they provide; in general, no or limited functional aspects of the network are modelled. Complex network theory methods can be applied to the analysis of CIs for i) helping to identify preliminary vulnerabilities by topology-

driven and dynamical analyses and ii) guiding and focusing further detailed analyses of critical areas (Kröger and Zio, 2011).

Topological analysis based on complex network theory can unveil relevant properties of the structure of a network system (Albert et al., 2000; Strogatz, 2001) by i) highlighting the role played by its components (Crucitti et al., 2006; Zio et al., 2008) and ii) making preliminary vulnerability assessments based on the simulation of failures (mainly represented by the removal of nodes and arcs) and subsequent re-evaluation of the network topological properties (Rosato et al., 2007; Zio et al., 2008). Notable studies concerned with the structural analysis and assessment of the vulnerability among the CIs sector include structural vulnerability of urban transport networks (Jenelius, 2009, Masucci et al., 2009), vulnerability of power grids (Bompard et. al 2009, Crucitti et al. 2005, Holmgren 2006, Hines and Blumsack, 2008, Eusgeld et al., 2009), and the Internet links (Latora and Marchoiri, 2005). Although simple graph models are common ways to represent and analyze CI networks, parts of physical properties can also be incorporated into the structure representation of realistic CI systems (e.g., electrical power infrastructure) (Hines and Blumsack, 2008; Cotilla-Sanchez et al., 2012).

Further, in real CI networks, another importance dimension to add to the vulnerability characterization is the *dynamics* (i.e., processes going on within networks) of flow of the physical quantities in the network. This entails considering the interplay between structural characteristics and dynamical aspects, which makes the modeling and analysis very complicated, since the load and capacity of each component, and the flow through the network are often highly variable quantities both in space and time (Kröger and Zio, 2011). *Percolation* theory, borrowed from physics, provides a useful tool for the rigorous treatment of network dynamics. It describes the process in which vertices or links on a network are randomly designated "occupied" or "unoccupied". Site percolation and bond percolation indicates the state of network nodes and links, respectively (Grimmett, 1999). This idea has been extended to address fundamental dynamic processes such as cascading failures in CI networks - where failure is the "occupied" state (Buldyrev et al., 2010; Xiao et al., 2011).

Functional models have been developed to capture the basic dynamic features of CI networks within a weighted topological analysis framework (e.g., Motter and Lai, 2002; Motter, 2004; Dobson et al., 2005c). These abstract modelling paradigms allow analyzing the system response to cascading failures and can be used to guide a successive detailed simulation focused on the most relevant physical processes and network components. The need for such an analysis tool is even stronger for systems in which the cascade dynamics is rapid and modifications are actuated on to the network in order to mitigate the evolution of the cascade. For example, cascading events leading to a blackout in power grids usually occur on a time scale of minutes to hours and is completed in less than one day (Dobson et al., 2007). Despite their apparent simplicity, these models provide indications on the elements criticality for the propagation process (Zio and Sansavini, 2011a) and on the actions that can be performed in order to prevent or mitigate the undesired effects (Motter, 2004).

2.1.2 Network representation of CI systems

Network theory provides a natural framework for the mathematical representation of network CI systems. A graph consists of *vertices* (sometimes referred to as nodes), V, and *edges* (sometimes referred to as arcs or links), E, which together construct a *graph*, $G(V, E)$ (see Figure 2:1). The number of vertices and edges are normally denoted as N and M, respectively. The network structure is usually represented by a $N \times N$ *adjacency matrix* A, where $A_{ij} = 1$ if there is an edge between vertices i and j, i.e. $(i, j) \in E$, and $A_{ij} = 0$ if there

is no edge between the two vertices, i.e. $(i, j) \notin E$. Normally, a vertex cannot have an edge to itself, i.e. $A_{ii} = 0$, and only one edge can exists between any two vertices. If these constraints are not fulfilled the graph is termed a *multigraph*. A graph can be directed or undirected. A directed edge is normally termed *arc*. It is possible to assign values to the edges (or the vertices) representing properties of the edges (or the vertices) like costs, lengths, capacities, etc. Such graphs are referred to as a *weighted* or a *valued* graph. It is also possible to differentiate between types of vertices or types of edges (as done in the appended Papers [3], [4], [5] and [6] in Part II of this thesis). Throughout the dissertation, vertices/nodes and arcs/edges will be also referred to as *components*.

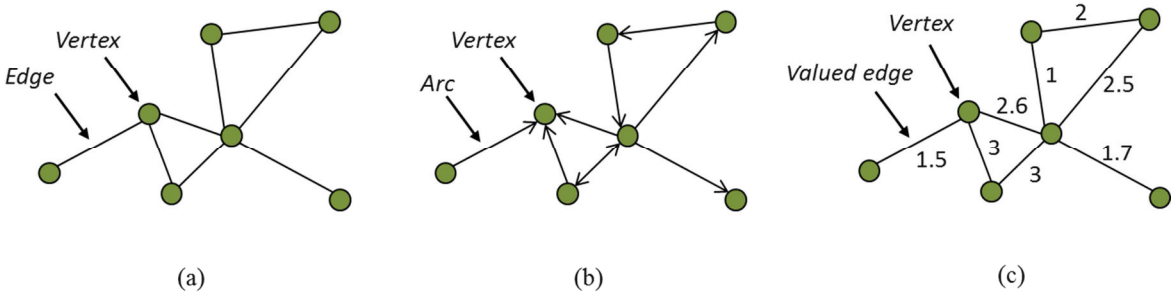


Figure 2:1 Example of (a) an undirected graph, (b) a directed graph, and (c) a weighted (valued) graph.

The idea behind network theory is the notion that it is possible to draw relevant conclusion about the modelled CI systems (e.g., electrical power grids, transportation networks, the Internet, etc.), by knowledge of its topology, as represented by a graph. By analyzing the structure of the network or by quantifying properties of the network when it is changed or, by some means, degraded, interesting properties of the system can be found.

There are a number of concepts and metrics with the aim to describe and measure the static structure of a network: a few of the most commonly used and relevant ones are summerized in Table 2:1.

Table 2:1 Brief overview over concepts and metrics used in complex network theory.

Concept	**Description**
Path	Defined as a sequence of vertices $\{v_1, v_2, \ldots, v_n\}$ such that $A(v_i, v_{i+1}) = 1$, i.e. there is an edge (v_i, v_{i+1}) for every i. A path where no vertex appears twice is called an *elementary path*.
Length	Describes the number of edges in a path, which is equal to the number of vertices in the path minus one.
Shortest path (geodesic)	A path starting in vertex, i, and ending in vertex, j, with the smallest possible length is called *geodesic* between i and j.
Degree of vertex i	The number of edges connected to the node i. If the graph is directed, one differentiates between *in-degree*, number of arcs coming into the vertex, and *out-degree*, number of arc coming out from the vertex. The average degree of i is simply the arithmetic mean of the degree for all vertices, i, belonging to G.

Metric	Description	Quantification
Distance	Distance is simply the length of a geodesic between i and j.	d_{ij}
Degree centrality, $C^D(v)$	The degree of a vertex, v, normalized over the maximum number of neighbors this vertex could have.	$C^D(v) = \frac{k(v)}{N-1}$
Betweenness centrality, $C^B(v)$, $C^B(e)$	A measure that tries to capture the importance of a vertex, v, or edge, e, in a network (Freeman, 1979). It describes how many shortest paths, geodesics (σ), that goes through a specific vertex or edge.	$C^B(v) = \sum_{i \neq j \neq v \in V} \frac{\sigma_{ij}(v)}{\sigma_{ij}}$ $C^B(e) = \sum_{i \neq j \in V} \frac{\sigma_{ij}(e)}{\sigma_{ij}}$
Closeness centrality, $C^C(v)$	A measure the idea of speed of communication between vertices in a way that the vertex that is "closest" to all others received the highest score (Zio and Sansavini, 2011a). The closeness of a vertex v is defined as the reciprocal of the average shortest path length.	$C^C(v) = \frac{1}{avg(d_{ij})}$ $= \frac{N-1}{\sum_{j \in V} d_{ij}}$
Clustering coefficient, C	Describes how clustered the network is in form of the density of triangles in the network (Watts and Strogatz, 1998). N is the number of vertices, C_i is the local clustering coefficient, M_i is the number of edges that exist between the neighbors of vertex i, and k_i is the number of neighbors for vertex i	$C = \frac{1}{N} \sum_{i \in V} C_i$ $= \frac{1}{N} \sum_{i \in V} \frac{M_i}{k_i(k_i-1)/2}$
Efficiency	A measure of efficiency in the communication between i and j, defined as inversely proportional to the shortest distance.	$\varepsilon_{ij} = \frac{1}{d_{ij}}$
Characteristic path length	The average distance of a graph, i.e. the average of the shortest distance d_{ij} between all pairs of vertices.	$L = \frac{1}{N(N-1)} \sum_{i \neq j} d_{ij}$
Network (average) efficiency, $E(G)$	A measure of how efficiently the whole network exchanges information (Latora and Marchiori, 2001).	$E(G) = \frac{1}{N(N-1)} \sum_{i \neq j} \varepsilon_{ij}$
Information centrality, $C^I(v)$	The information centrality of a vertex, v, is defined as the relative drop in the network efficiency caused by the removal from G the edges incident in v (Latora and Marchiori, 2007).	$C^I(v) = \frac{\Delta E(v)}{E}$ $= \frac{E[G] - E[G'(v)]}{E[G]}$

In the network theory framework, CI system failures are normally represented topologically as the removal of vertices and edges. There are different failure initiating strategies that usually based on a random process or by

using some measurement of the *importance* of components and then removing these in a certain order. The *importance* is usually based on a *centrality measure*, which aim to qualify the role played by a component in the complex interaction and communication occurring in the network. Classical topological centrality measures are the degree centrality, the closeness centrality, the betweenness centrality and the information centrality (see Table 2:1) (Freeman, 1979; Latora and Marchiori, 2007).

2.2 Hierarchical network representation framework

2.2.1 Clustering techniques

Recent studies suggest that many real complex networks exhibit a modularized organization (Porter et al., 2009). In many cases, these modularized structures are found to correspond to functional units within networks (ecological niches in food webs, modules in biochemical networks) (Karrer et al., 2008). Broadly speaking, clusters (also called communities or modules) are found in the network, forming groups of elements that are densely interconnected with each other but only sparsely connected with the rest of the network. The study of the clustered structure of the network of a CI is of particular interest because such structure can provide itself a protection for the system against attacks from an intruder (Eum et al., 2008), reduce the effects of cascading failures (Wu et al., 2006) and point at important heterogeneities within the network that may not be registered via network level measures (Karrer et al., 2008).

Clustering aims at identifying patterns around which communities of elements in the network can be grouped, emerging implicit information in the network structure (Filippone et al., 2008). Framed as an unsupervised multiple classification problem (Schölkopf et al., 1998), clustering has been an essential undertaking in the context of explorative data mining and also a common technique for statistical data analysis used in many fields such as machine learning, pattern recognition, image analysis, information retrieval, and bioinformatics (Jain et al., 1999). Theoretically, based on a similarity (affinity) measure s_{ij} between pairs of data points (i, j), which is usually a measure of distance between i and j, most clustering approaches seek to achieve a minimum or maximum similarity value through an iterative process of vertex grouping (Filippone et al., 2008; Gómez et al., 2011). Different similarity definitions can lead to different cluster partitioning of the network.

For the detailed description of the different clustering methods, the reader is encouraged to refer to Filippone et al. (2008) and Jain et al. (1999). For the purpose of the clustering analysis in this research, the unsupervised spectral clustering algorithm (USCA) (Von Luxburg, 2007) is adopted, which is invariant to cluster shapes and densities and simple to implement. The USCA makes use of the spectrum (eigenvalues) of the similarity matrix of the data to perform dimensionality reduction before Fuzzy k-Means (FKM)-clustering in fewer dimensions. Schematically, it is performed by the steps presented in Table 2:2 (Von Luxburg, 2007).

In the first step, the Laplacian matrix L_{sym} is calculated from the similarity (affinity) matrix as follows. The input similarity matrix S is of size $n \times n$ and its generic element s_{ij} represents the similarity between nodes i and j in the network. The diagonal components s_{ii} are set to 1 and the matrix is symmetric($s_{ij} = s_{ji}$). The degree matrix D is the diagonal matrix with diagonal entries $d_1, d_2, \ldots, d_n$ defined by

$$d_i = \sum_{j=1}^{N} s_{ij}\,, i = 1,2,\dots,n \tag{2.1}$$

Then, the normalized graph Laplacian matrix can be obtained:

$$L_{sym} = D^{-1/2} L D^{-1/2} = I - D^{-1/2} S D^{-1/2} \tag{2.2}$$

where $L = D - S$ and I is the identity matrix of size $n \times n$.

Table 2:2 The unsupervised spectral clustering algorithm.

Input:	Similarity matrix $S \in \mathbb{R}^{n \times n}$
1.	Compute the normalized graph Laplacian matrix L_{sym}.
2.	Compute the first k eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_k$ and corresponding eigenvectors $\overline{u}_1, \overline{u}_2, \dots, \overline{u}_k$of matrix L_{sym}. The first k eigenvalues are such that they are very small whereas λ_{k+1} is relatively large. All eigenvalues are ordered increasingly.
3.	The number of clusters is set equal to k, according to the eigengap heuristic theory
4.	Let $U \in \mathbb{R}^{n \times k}$ be the matrix containing the vectors $\overline{u}_1, \overline{u}_2, \dots, \overline{u}_k$ as columns. Form the matrix $T \in \mathbb{R}^{n \times k}$ from U by normalizing the rows to norm 1, that is set $t_{ij} = u_{ij} / \left(\sum_k u_{ik}^2\right)^{1/2}$.
5.	For $i = 1, \dots, n$, let $y_i \in \mathbb{R}^k$ be the vector corresponding to the i-th row of T
6.	Resort to the FKM algorithm to partition the data points $(y_i)_{i=1,\dots,n}$ into k clusters $A_1, \dots, A_k$
Output:	Clusters $C_1, \dots, C_k$ with $C_i = \{j \vert y_j \in A\}$

It should be noted that the eigengap heuristic theory at the basis of the third step of the algorithm works well when the modularized structure of the data are pronounced whereas the more noisy or overlapping the clusters are, the less effective it is (Von Luxburg, 2007). In those cases, other methods such as the Markov clustering algorithm (Van Dongen, 2000) can be used to find the optimal number of clusters.

2.2.2 Hierarchical network representation

Hierarchically modularized organization, which is a central idea about the life process in biology, is found to be also an internal structure of many technique networks (Sales-Pardo et al., 2007), and can be utilized to model these complex systems for the management of system complexity (Gómez et al., 2011).

For illustration of the potential of the hierarchical modelling framework for complex system analysis, by analogy one may think of the electronic maps such as those provided by Google Maps; the tools are powerful because they present information in a scalable manner – despite the decrease in the amount of information as we "zoom in", the representation shows the information that is relevant at the new scale.

In the same spirit, a hierarchical model representing the whole system at the top and individual elements at the bottom could be obtained via a process of successive clustering of the network and network subsystems (e.g., via successively performing the USCA on the network). Then, based on the hierarchical network representation, fictitious networks can be defined in each level, from which the analyst can extract relevant information at the suitable level of the hierarchy. Fictitious networks are cluster-simplified representations of the real network and can facilitate the understanding and analysis of the network properties by focusing on the relevant information that emerges at the different levels.

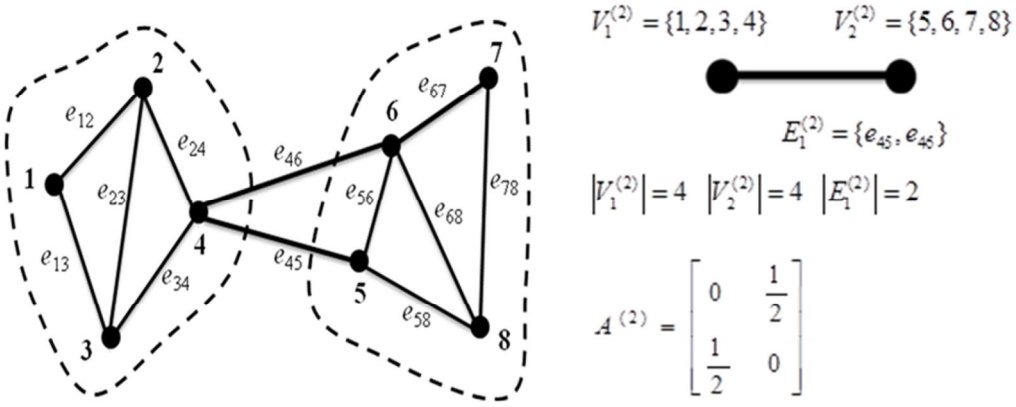


Figure 2:2 Illustrative example of the construction of fictitious networks.

Specifically, the artificial network at level l of the network hierarchy is described as a graph $G^{(l)}(\Lambda^{(l)}, E^{(l)})$ with $1 \le l \le L$, where L is the number of levels of the hierarchy. We use $V_i^{(l)}$ to represent the artificial node i (for $i = 1,2,\dots,|\Lambda^{(l)}|$) at level l, which corresponds to a cluster of real network nodes. Artificial nodes are connected by artificial links $E_{ij}^{(l)}$ (for $i,j = 1,2,\dots,|\Lambda^{(l)}|$ and $i \neq j$), composed by those actual network links connecting (in parallel) the actual nodes in the clusters forming the artificial nodes, $E_{ij}^{(l)} = \left\{ e_{st} \middle| v_s \in V_i^{(l)}, v_t \in V_j^{(l)} \right\}$. The connection pattern between artificial nodes at level l is illustrated by an *adjacency matrix* $\boldsymbol{A^{(l)}}$ whose element $A^{(l)}\left(V_i^{(l)}, V_j^{(l)}\right) = 1/\left|E_{ij}^{(l)}\right|$ if $E_{ij}^{(l)} \neq \emptyset$, i.e. if in the artificial nodes $V_i^{(l)}$ and $V_j^{(l)}$ are connected by fictitious edge $E_{ij}^{(l)}$ and 0 otherwise. This definition accounts for the fact that a fictitious edge embracing several real links has that number of paths available between the two communities it connects, thus holding more interaction efficiency and smaller weight viewed as the *physical distance* between the two communities connected by the virtual edge. Figure 2:2 gives an example of the construction of a fictitious network.

The hierarchical modelling framework offers different levels of resolution at the different levels of the hierarchy. The artificial networks at the top of the hierarchy contain limited detail information of the local connectivity patterns (in the limit, only one node represents the whole network at the first level of the hierarchy); as we move down the hierarchy, more local information enters the model, at the expense of an increase in the dimension of the network. These characteristics can be leveraged efficiently to facilitate the management of complexity in the analysis of large-scale CI systems. In Chapter 5 and appended Papers [1] and [2], we will illustrate this by referring to the vulnerability and reliability analysis of a realistic CI network, i.e. the 380kV Italian Power Transmission Network (IPTN380).

2.3 Extended reliability-based component importance measures

Component importance measures (CIMs) are widely used in system engineering to identify components within the system that most significantly influence the system behavior with respect to reliability, risk and/or safety. The indications drawn are valuable for establishing direction and prioritization of actions, related to reliability improvement during system design and optimization of operation and maintenance.

A well-known CIM is the so called Birnbaum IM defined as (with reference to system reliability R_s, as the system performance indicator) (Birnbaum, 1968):

$$I_i^B = \frac{\partial R_s}{\partial R_i} = R_s(R_i = 1) - R_s(R_i = 0) \tag{2.3}$$

where I_i^B is the Birnbaum Importance (BI) of component i; R_s represents the reliability of the system; R_i is the reliability of component i; $R_s(R_i = 1)$ is the system reliability calculated assuming that component i is perfectly operating and $R_s(R_i = 0)$ the system reliability in the opposite case of component i failed. The BI measures the significance of component i to system reliability by the rate at which system reliability improves with the reliability of component i. As shown in Equation (2.3), the BI of component i does not depend on R_i itself, so that two components i and j may have a similar value I^B although they have different reliability values R_i and R_j, respectively; this could be seen as a limitation of BI.

The Criticality Importance (CImp) measure overcomes the above limitation by considering component unreliability (Espiritu et al., 2007). It is defined as:

$$I_i^C = I_i^{BI} \frac{F_i}{F_s} = [R_s(R_i = 1) - R_s(R_i = 0)] \frac{1 - R_i}{F_s} \tag{2.4}$$

where F_i is the unreliability of component i and F_s is the system unreliability. Now, a less reliable component is more critical than another one with same value of BI.

Fuessell & Vesely (Fussell, 1975) proposed an alternative importance measure according to which the importance of a component in the system depends on the number and on the order of the cut sets in which it appears. Most commonly used as a risk reduction indicator, Fuessell & Vesely Importance (FVI) quantifies the maximum decrement in system reliability caused by a particular component being failed ($R_i = 0$):

$$I_i^{FV} = \frac{R_s - R_s(R_i = 0)}{R_s} \tag{2.5}$$

The previously proposed CIMs (BI, CImp and FVI) are functionally different. They evaluate subtly different properties of the system behavior, and therefore, are often used in a complementary fashion to infer different information. However, in order to apply the CIMs for analyzing a CI network system such as the IPTN380, it is necessary to extend the definition of the CIMs to account for the multiple terminal or node pairs (e.g. generator-distributor pairs) where connectivity defines the network functionality.

Specializing such extension for the analysis of the importance of components of a CI network system, we introduce the Extended Birnbaum Importance (EBI) measure as the average of all BI values obtained considering all possible Generator-Distributor pairs reliabilities in the network system:

$$I_i^{E-B} = \frac{1}{N_G N_D} \sum_{s \in V_G, d \in V_D} \frac{\partial R_{sd}}{\partial R_i} = \frac{1}{N_G N_D} \sum_{s \in V_G, d \in V_D} [R_{sd}(R_i = 1) - R_{sd}(R_i = 0)] \tag{2.6}$$

where N_G and N_D are the number of generators and distributors in the network respectively; V_G and V_D are sets of node generators and distributors respectively; R_{sd} is the terminal pair reliability (TPR) between node s and node d; $R_{sd}(R_i = 1)$ and $R_{sd}(R_i = 0)$ represent the terminal pair reliabilities between node s and node d, in the condition that component i is perfectly operating and completely failed, respectively.

Similarly, we can define Extended Criticality Importance (ECI) and Extended Fussell &Vesely Importance (EFVI) measures:

$$I_i^{E-C} = \frac{1}{N_G N_D} \sum_{s \in V_G, d \in V_D} [R_{sd}(R_i = 1) - R_{sd}(R_i = 0)] \frac{1 - R_i}{1 - R_{sd}} \tag{2.7}$$

$$I_i^{E-FV} = \frac{1}{N_G N_D} \sum_{s \in V_G, d \in V_D} \frac{R_{sd} - R_{sd}(R_i = 0)}{R_{sd}} \tag{2.8}$$

where I_i^{E-C} is the Extended Criticality Importance (ECI) measure of component i and I_i^{E-FV} is the Extended Fussell &Vesely Importance measure.

The definitions in formulas (2.6)-(2.8) render CIMs compatible and applicable to a complex distributed network system, providing risk managers with information on the risk/safety significance of system structures and components. However, their computation in large or even moderate network systems is non-trivial. In Chapter 5 and appended Paper [2], we will illustrate how the hierarchical modeling introduced in the previous Section can be used to set up a framework within which the extended CIMs of the components of large-scale complex network systems can be computed efficiently, due to the multi-scaled information representation scheme.

Chapter 3 CI optimization against cascading failures

As introduced in Chapter 1, systemic risk leads to catastrophic impact in a way of *cascading failure*, and its occurrence is much more likely than might be expected: for example, the probability distribution of blackout size happened in power grids approximately follows a power law, rather than an exponential type distribution predicted by traditional risk analysis (Chen et al., 2005; Dobson et al., 2007; Hines et al., 2009). This chapter addresses the problem of cascading (systemic) failures mitigation for CI networks by network optimization. Specifically, the problem is taken from a holistic system design perspective: some system properties, such as its topology and link capacities, are redesigned in an optimal way in order to enhance system's ability of *resisting* to cascading failures.

This Chapter starts with an overview of the existing studies about cascading failures in CI networks (Section 3.1). Then, the two different approaches of increasing complexity have been used to model cascading failures, i.e. a topological complex network-based model and a physical flow-based model (for electrical power grids), are summarized (Section 3.2). Finally, this problem of redesigning network properties (e.g., topology and link capacities) to increase network resistence to cascading failures is formulated within a multi-objective optimization framework, and is solved by evolutionary algorithms (Section 3.3).

3.1 Cascading failures in CI networks

Cascading failure is the usual mechanism by which failure propagates to cause large outages of CI networks, such as power the electrical power transmission networks (U.S.-CA, 2004; U.C.T.E, 2004; 2007; Pidd, 2012), the Internet (Newman et al., 2002) and financial networks (Battiston et al., 2007). It is defined as "*a sequence of dependent failures of individual components that successively weakens the system, usually initiated by a disturbance or trigger events*" (Baldick et al., 2008).

While cascading phenomena have a diversity of failures and many different mechanisms by which failures can propagate, *load redistribution* plays a key role in the process of failure propagation (Motter, 2004; Simonsen et al., 2008). In the cascading failures taking place on the Internet, traffic is rerouted to bypass malfunctioning routes, eventually leading to an avalanche of overloads on other routers that are not equipped to handle extra traffic. The redistribution of the traffic can result in a congestion regime with a large drop of the performance (Guimera et al., 2002; Crucitti et al., 2004). When cascading failures happen in electrical power grids, the power of a (for any reason) failed line is automatically shifted to the neighboring lines, which in most of the cases are able to handle the extra load. Few times, however, also these lines are overloaded and must redistribute their increased load to their neighbors. This eventually leads to a cascade of failures: a large number of transmission lines are overloaded and malfunction in a very short time period.

In the past two decades, a large volume of work has been devoted to understanding and analyzing cascading failures, differing for both the logic of failure propagation and the extent to which they abstract the underlying physical CI systems. A review of different available methods for analyzing cascading failures specifically in power grids is provided by Baldick et al. (2008). These efforts can be categorized into three classes: (i) (high-

level) probabilistic analytical models, (ii) simulation and models selecting and approximating a modest subset of the many physical and engineering mechanisms of cascading failure, and (iii) an extensive complex literature on cascading in abstract networks.

(High-level) Probabilistic approaches for cascading failures tend to capture the stochastic dynamics of cascading failures without detailed models of the interactions and dependencies. They provide insight into the general qualitative features of cascading failures such as the risk of cascading failure, probability distribution of the outage size and the asymptotic behavior of cascading failures in certain cases. The CASCADE model by Dobson et al. (2005a) models cascading failures triggered by initial load increments on certain components of the system. In this model, failures occur due to overloaded components and cascading failures develop as a result of redistribution of loads among the remaining components. However, the redistribution of loads is based upon simple assumptions; for example, loads are added equally to the components of the system as a result of failures.

Probabilistic models based on branching processes (Dobson et al., 2005b; Ren and Dobson, 2008; Dobson, 2012) have also emerged, providing a framework for studying the statistical properties of cascading failures, such as the probability distribution of the failure size. These approaches model cascading failures by considering generations of failures, whereby each failure in each generation independently produces a random number of subsequent failures in the network generation, and so on. Branching process-based approaches have the limitation that they do not have sufficient degree of freedom to capture the effect of physical factors contributing to cascading failures, as the failure generation parameter is the only parameter used in these models.

Simulation and models with a modest subset of physical attributes: There are many simulations and models of cascading failure using Monte Carlo and other methods, selecting and approximating a modest subset of the many physical and engineering mechanisms of the system under study. Taking the study of cascading failures in electrical power grids as an example, the so-called Manchester model (Nedic et al., 2006) is a fairly detailed blackout model based on AC power flow simulation. The Hidden failure model (Bae and Thorp, 1999; Chen et al., 2005; Wang and Thorp, 2001) is based on the hidden failure theory and tends to simulates hidden relay failures probabilistically, taking into account the DC power flow constraint of the network.

In addition, some researchers (Iyer et al., 2009; Wang et al. 2012) provide Markov-transition models for cascading failure in power grids, where the transition probabilities among states are derived from a stochastic model of line overloading based on a stochastic flow redistribution model based upon DC power-flow equations. However, the state space of Markov-based model is large, as it requires tracking the functionality status of transmission lines and power flow information; in addition, due to the analytical complexity of the time-varying transition probabilities, the analytical and asymptotic characterization of probabilistic metrics, such as the blackout probability and distribution of the blackout size, is not possible.

Researchers at Oak Ridge National Laboratory (ORNL), Power System Engineering Research Center of Wisconsin University (PSerc), and Alaska University (Alaska) have proposed a landmark study for blackout modelling in power grids, called the ORNL-PSerc-Alaska (OPA) model (Dobson et al., 2001). The OPA model is built upon the Self-Organized Criticality (SOC) theory and DC power flow attributes, contains two different time scale dynamics (i.e., power flow dynamics and power grid growth dynamics), and reveals the complexity and criticality of power systems. Based on the OPA model, it is found that operation near critical points can

produce power law tails in the blackout size probability distribution, similar to those observed in the analysis of 15 years of North American blackout data (Sachtjen et al., 2000; Dobson et al., 2007; Hines et al., 2009). Only ideal cases, such as tree networks, and real networks with a small number of nodes (~ 100) have been considered by Carreras et al. (2002). Large networks and the influence of the topology on the dynamics of the model have not been studied yet.

Network theory approaches: There is an extensive literature on cascading failures in abstract networks that has been originally motivated in part by the propagation of failures and congestion in the Internet (Watts, 2002; Motter and Lai, 2002; Holme et al., 2002; Motter, 2004; Crucitti et al., 2004; Kenney et al., 2005; Li et al., 2013). The dynamics of the cascade is related to statistical topological properties of the networks. Some researchers (e.g., Albert et al., 2000; Holme et al., 2002) have studied the response of complex networks under different attack strategies; however, the dynamics of failure propagation has not been considered.

Motter and Lai (2002) have introduced a simple but sophisticated model (referred to as the ML model hereafter) for cascades of overload failures in networked systems (e.g., the Internet and power grids), based on the concept of betweenness centrality. The model shows how an even small fraction of highly loaded nodes can trigger global cascades in networks with heterogeneous distribution of loads. Based on this model, it has been shown that a strategy of defense relying on the selective removal of components right after the initial attack or failure and before the propagation of the cascade can constitute an efficient strategy of defense (Motter, 2004; Li et al., 2013).

Crucitti et al. (2004) have proposed a variation to the ML model in which, instead of permanently removing the overloaded nodes, the communication through these nodes is degraded, so that eventually the flow of the relevant quantities (information or energy) will avoid them. In this sense, the model can be considered as well as a model for congestion in communication networks. Kinney et al. (2005) have applied the model by Crucitti et al. (2004) to the study of cascading failures in the North American power grid and found that the loss of vertices with high load causes a higher damage in the system than the loss of random vertices. Simonsen et al. (2008) studied cascading failure in networks using a dynamical flow model which take into account the network topology, flow conservation, and the distribution of loads over the ne neighboring links of a node.

Some other studies have addressed the overload breakdown problem in time evolving networks. In fact, as the network changes, the load is redistributed: if this is not accounted for, it may trigger a node breaking avalanche. Holme et al. have proposed a model for breakdowns triggered by changing nodes (Holme and Kim, 2002) or edges (Holme, 2002) load in an evolving network. The results show the presence of cascading failures, and those are more violent when the network growth is ruled by preferential rather than random attachment. Wang and Xu (2004) have studied cascading failures in coupled map lattices (CML) and proposed a model based on coupled logistic maps in the chaotic regime and a failure threshold mechanism. The breakdown of a single node is sufficient to trigger an entire network to collapse if the amplitude of the external perturbation on the single node is larger than a given threshold. Furthermore, it has been found that the threshold for a globally CML is much larger than that for a small-world or scale-free CML. This implies that cascading failures occur much easier in small-world and scale-free networks than in global coupling networks.

3.2 Cascading failure modelling approaches in this study

As discussed in Section 3.1, cascading failure models based on Complex Network Theory abstract the representation of physical infrastructures as graphs and study the connectivity characteristics, the propagation mechanisms through the graph connections and their relationships. These types of models have proved to provide a good understanding of the specific dynamics of cascading failures (Holmgren, 2006). They have the advantage of modelling cascading dynamics with few parameters, so that its application to realistic, large-scale networks is feasible and certainly easier (Kenney et al., 2005).

However, negative accounts on these abstract models do exist, especially when applying to electrical power infrastructures (which are among the most important infrastructure networks, and will be the focus of this study). For example, Fitzmaurice et al. (2012) find that the topological nearest neighbor cascading failure model (namely, the TC model) shows characteristics that are different from two other Kirchhoff models, namely the linear dynamic (LD) model and the quasi-steady state (QSS) model. Hines et al. (2010) conclude that evaluating vulnerability in power networks using purely topological metrics may be misleading under some circumstances.

For these reasons, in this study, both a representative Complex Network Theory-based model (i.e. the ML model, Section 3.2.1) and a representative physical power flow-based model (the OPA model, Section 3.2.2) are embraced for cascading failure simulation in electrical power grids and systematically compared.

3.2.1 The ML model

The ML model assumes that at each time step, one unit of the relevant quantity (e.g., electrical flow for power grids) is exchanged between every pair of generation and demand nodes, and transmitted along the shortest path connecting them. Then, the flow at one link is computed as the number of shortest paths passing through it. More precisely, the flow F_l^{ML} of link l is quantified by the link betweenness, calculated as the fraction of the generator-distributor shortest paths passing through that link:

$$F_l^{ML} = \frac{1}{N_G N_D} \sum_{i \in V_G, j \in V_D} \frac{n_{ij}(l)}{n_{ij}}, l \in E \tag{3.1}$$

where E is the set of all the links in the network; V_G ($\|V_G\| = N_G$) and V_D ($\|V_D\| = N_D$) are the sets of generation and demand nodes, respectively; n_{ij} is the number of shortest paths between generation nodes and demand nodes, and $n_{ij}(l)$ is the number of generation-demand shortest paths passing though link l.

In the *original* ML model (Motter and Lai, 2002), a homogeneous capacity-load relationship is assumed: the capacity of link l is assumed to be proportional to its initial flow $F_l^{ML}(0)$ with a network tolerance parameter α:

$$C_l^{ML} = (1+\alpha) F_l^{ML}(0), l \in E \tag{3.2}$$

The concept of tolerance parameter α ($\alpha \geq 0$) can be understood as an operating margin allowing safe operation of the component under potential load increment. The occurrence of a cascading failure is initiated by removal of a link, which in general changes the distribution of shortest paths. Then, the flow at a particular link can change and if it increases and exceeds its capacity, the corresponding link fails. Any failure leads to a new redistribution of loads and, as a result, subsequent failures can occur.

The detailed simulation of the ML cascading failure model proceeds as follows:

1) A random link is chosen as failed and, thus, is removed from the network.
2) Recur to Equation (3.1) and Floyd's shortest paths algorithm to calculate the flow of each working link in the network.
3) Test each link for failure: for each link $l \in E$ of the network, if $F_l^{ML} > C_l^{ML}$ then link l is regarded as failed and, thus, is removed from the network.
4) If any working link fails, return back to step 2. Otherwise, terminate the simulation and evaluate the network damage.

More details of the ML model can be found in Motter and Lai (2002) and appended Papers [3], [4].

3.2.2 The OPA model

The cascading failure model is based on the standard DC power flow equation,

$$F^{OPA} = A \cdot P \tag{3.3}$$

where F^{OPA} is a vector whose M components are the power flows through the lines, $F_l^{OPA}(l \in E)$, P is a vector whose $N-1$ components are the power injection of each node, P_i (N is the total number of nodes in the network), with the exception of the reference generator, P_0, and A is a constant matrix that depends on the network structure and impedances (see Ref. [10] for details about the computation of A). The reference generator power is not included in the vector P to avoid singularity of A as a consequence of the overall power balance.

The generator power dispatch is solved using standard linear programming methods. Using the input power demand, the power flow Equation (3.3) is solved with the condition of minimizing the following cost function:

$$f = \sum_{i \in V_G} P_i(t) + K \sum_{j \in V_D} P_j(t) \tag{3.4}$$

This definition gives preference to generation shift whilst assigning a high cost (set K =100) to load shedding, and it is assumed that all generators operate at the same cost and that all loads are served with equal priority. The minimization is done with the following constraints:

(1) Generator power injections are generally positive and limited by installed capacity limits: $0 \leq P_i \leq P_i^{max}, i \in V_G$.
(2) Loads always have negative power injections: $P_j^{dem} \leq P_j \leq 0, j \in V_D$.
(3) The flow through links is limited by link capacities: $\left|F_l^{OPA}\right| \leq C_l^{OPA}$.
(4) Total power generation and consumption remain balanced: $\sum_{i \in V_G \cup V_D} P_i = 0$.

After solving the linear optimization, we examine which lines are overloaded. A line is considered to be overloaded if the power flow through it is within 1% of the limit capacity C_l^{OPA}. Each overloaded line may outage with probability p_1 (p_1 is set as 1 in the case study in Chapter 5 to ensure its comparability with ML). If an overloaded line experiences an outage, its power flow limit C_l^{OPA} is divided by a very large number k_1 to ensure that practically no power may flow through the line. Besides, to avoid a matrix singularity from the line outage, the impedances of failed lines are multiplied by a large number k_2, resulting in changes of the network

matrix A. Similary, for more details of the OPA model, one can refer to Dobson (2001) and to appended Papers [3], [4].

3.3 Network optimization against cascading failures

Cascading failures are manifestation of the potential vulnerability of otherwise highly robust networks (such as the power grids) due to the interdependency between the successive events. Reliability improvement efforts (such as critical parts upgrading) are unlikely to eliminate all failures, and future cascading failures in CIs are inevitable (Talukdar et al., 2003). Therefore, an essential question is, then, how to enhance CI *survivability* even if cascading failures happen. This question is here addressed from a holistic system design perspective, i.e. some system parameters (such as its topology and link capacities) are redesigned in an optimal way to enhance system's robustness against cascading failures.

3.3.1 Topology optimization

Albert et al. (2004) demonstrated that the vulnerability of modern infrastructure networks (e.g., power transmission networks) is inherent to their structure. Thadakamalla et al. (2004) revealed that the topology of a supply infrastructure has great impact on its resilience. Then, much attention has been paid in recent years in the direction of network topology optimization, with the purpose of achieving desired targets of reliability and/or robustness (Shao et al., 2005; Gutfraind, 2010; Ash and Newth, 2007).

In practical cases, the cost of knocking down an existing network and reconstructing it from scratch is prohibitive, especially for CIs like the power transmission network. A more practicable alternative is to reconfigure parts of the network topology, e.g. by reallocation of the links which connect production facilities to consumers.

Consider a weighted undirected graph G with a set of N nodes representing N_g power generators and N_d loads representing distribution substations, interconnected by a set of edges representing transmission lines. The structure of the network is identified by its adjacency matrix W. The weight of the edge between i and j is given by their physical distances $d(i,j)$, which we assume directly related to the transmitting cost of the link. We define the variables to be optimized as the links of generation nodes to the different distribution nodes:

$$X_{ij} = \begin{cases} 1, if\ i\ is\ connected\ with\ j\ directly \\ 0, \qquad\qquad\qquad\qquad otherwise \end{cases} \tag{3.5}$$

for all $i \in V_g$ and $j \in V_d$. Two constraints have to be met when rewiring generators and distributors: (1) each distributor node is required to connect with at least one generator node or other distributor node, to make it accessible to the power supplying generators; (2) each generator node has to connect at least with one distributor node.

We assume that the cost associated with each connection cutting and rewiring is linearly proportional to the physical length of the linkage, with coefficient φ. The total investment cost of a reconstructed pattern X in the power transmission network can be defined as

$$Cost(X_{ij}) = \sum_{i \in V_G j \in V_D} \varphi X_{ij}\, d(i,j) \tag{3.6}$$

where $d(i,j)$ is the physical distance between i and j.

For each reconstructed pattern X, the computationally-cheap ML model is here used to simulate and quantify the network *vulnerability* to cascading failures, which is characterized by the fraction of network (average) efficiency lost in the cascading failure

$$Vul(G) = \frac{E(G) - E(\overline{G})}{E(G)} \tag{3.7}$$

where $Vul(G) \in (0, 1)$, $\overline{G}$ represents the residual network structure after the simulation of cascading failure (introduced in Section 3.2.1) achieving and maintaining a stable state, and $E(G)$ is the network (average) efficiency defined in Table 2:1.

It should be noted that the effect of the type of initial event could significantly influence the cascading failure result: the efficiency loss of a cascade triggered by the failure of a critical component could be much more severe than that originated by the failure of a normal component. Therefore, in this study we consider a *worst-case* scenario by choosing the failure of one of the top five most loaded nodes as initial failure in each cascade process simulation and, then, we average the results are averaged on the number of simulations.

Through the quantification of the connection pattern cost and cascading failure vulnerability, the facility allocation problem is formulated as a multi-objective optimization problem:

$$\begin{cases} \min Cost(X_{ij}) & \text{(3.8a)} \\ \min Vul\left(Q_{X_{ij}}\right) & \text{(3.8b)} \end{cases}$$

$$s.t. \begin{cases} \sum_{i \in V_g \cup V_d} X_{ij} > 0 \ \forall j \in V_d & \text{(3.8c)} \\ \sum_{j \in V_d} X_{ij} > 0 \ \forall i \in V_g & \text{(3.8d)} \end{cases}$$

The objective function (3.8a) is the sum of the fixed rewiring costs (to be minimized); (3.8b) expresses the objective of maximizing network robustness against cascading failures (i.e., minimizing its vulnerabiltiy). Formulas (3.8c) and (3.8d) represent the two contstaints mentioned above (i.e., each distributor node is required to connect with at least one generator node or other distributor node, to make it accessible to the power supplying generators, and each generator node has to connect at least with one distributor node, respectively). Observe that the least costly generator allocation is simply that with no links among facilities and consumers. Finally, notice that in this analysis, *only* the computationally-cheap ML is *directly* used in the optimization process; the optimal topology hereby obtained is then *validated* only a *posteriori* by means of the OPA model. The reader is referred to appended Paper [3] for further details.

3.3.2 Capacity allocation optimization

Various problems concerning the robustness and functionality of CI systems (ranging from power outages and Internet congestion to affordability of public transportation) are ultimately determined by the extent to which the CI capability matches supply and demand under realistic conditions (Kim and Motter, 2008a). Actually, overloading is the most direct cause of failure propagation in a cascading failure. Then, the question is how to augment the capacities of components in a CI network in an effective manner in order to enhance its robustness against cascading failure, i.e., which type of capacity allocation pattern is the most robust against cascading failure.

In the study of cascading failure in CIs, a homogeneous capacity-load relationship has been widely used (Motter and Lai, 2002; Crucitti et al., 2004; Motter, 2004; Zio and Sansavini, 2011a; Li et al., 2013), whereby the capacity of a component is assumed to be proportional to the initial flow of the component. However, it has been argued by Kim and Motter (2008a) that this is unrealistic and empirical data suggests that the relationship between capacity and load of transmission lines is non-linear (Kim and Motter, 2008a; 2008b): heavily loaded lines usually have a lower tolerance parameter than lightly loaded lines. Wang and Kim (2007) proposed a (non-linear) two-step function for the relationship between the capacity and load of network vertices. Although based on an over-simplified model, it has been shown efficient to prevent cascades by protecting highest-load vertices. Li et al. (2008) introduced a more complex heuristic capacity model whereby vertices with both higher loads and larger degrees are paid more extra capacities. It is shown that this model can achieve better network robustness than previous models under the same amount of available resources.

In the present study, we tackle the issue from a systematic perspective by searching for the strategy of capacity allocation in a CI (power transmission) network that is most favorable for resisting to cascading failures, while keeping the total capacity limited (i.e., while minimizing the network cost). This is framed into a multi-objective optimization problem. In addition, notice that in this context, *both* the ML *and* OPA models are *directly* used in the optimization process and the corresponding optimal capacity patterns are found: then the results obtained are compared.

Specifically, we define the variables to be optimized as the capacities of the links in a network $G(V, E)$, $C_l, l \in E$ (namely, C_l^{ML} for the ML model and C_l^{OPA} for the OPA model). Thus, the homogeneous capacity allocation strategy originally used in the ML and OPA model, i.e. Equation (3.2), is no longer adopted in the optimization. Instead, any non-negative vector $C \in \mathbb{R}_+^M$ could represent a potential solution. It is noted that the searching space $\mathbb{R}_+^M$ is intractably large in reality, where a power transmission network usually has hundreds or thousands of links.

Similarly, the cost associated with each link capacity is assumed to be linearly proportional to the value of the capacity, with coefficient φ. The total investment cost related to a capacity allocation pattern $C \in R_+^M$ in the power transmission network can, then, be defined as:

$$Cost(C) = \sum_{l \in E} \varphi C_l \tag{3.9}$$

The network damage resulting from a cascading failure in the presence of a given capacity pattern can be obtained by running the cascading simulation (the ML or the OPA model) in correspondence of the capacity pattern and, then, using

$$Vul_{ML}(G_C) = \frac{E(G_C) - E(\overline{G}_C)}{E(G_C)} \tag{3.10}$$

(same as Equation (3.7)) when the ML model is adopted, or using

$$Vul_{OPA}(G_C) = \frac{LS}{D} = \frac{\sum_{j \in V_d} LS_j}{\sum_{j \in V_d} P_j^{dem}} \tag{3.11}$$

when the OPA model is adopted. Notice that P_j^{dem} and LS_j are the demand load and load shedding, respectively, at vertex j; D and LS represent the total load demand and load shedding, respectively, for the system. One can refer to the appended Papers [3] and [4] for the details of their calculations. The cascade simulations (ML and OPA) run over several iterations until they either converge or exceed the maximum number of steps. Finally, the network vulnerability for a given capacity allocation pattern C is obtained as the average network damage $\overline{Vul}_{ML}$ (or $\overline{Vul}_{OPA}$ for OPA), over various random triggers.

Through the quantification of the capacity allocation cost and cascading failure vulnerability, the capacity allocation problem is formulated as a multi-objective optimization:

$$\begin{cases} \min\limits_{C \in R_+^M} Cost(C) & \text{(3.12a)} \\ \min\limits_{C \in R_+^M} \overline{Vul}(G_C) & \text{(3.12b)} \end{cases}$$

The objective function (3.12a) is the sum of the link capacity costs (to be minimized); function (3.12b) expresses the objective of minimizing cascade vulnerability, where $\overline{Vul}(C)$ is $\overline{Vul}_{ML}(G_C)$ when the ML model is used, or $\overline{Vul}_{OPA}(G_C)$ when the OPA is used, respectively. Observe that under this definition the most cascade-resilient network might be the network with infinite capacity, which obviously would conflict with the objective of minimizing cost.

3.4 Evolutionary algorithms for network optimization

Multi-objective evolutionary algorithms (MOEAs) have proven to be general, robust and powerful search tools that are desirable for tackling problems involving i) multiple conflicting objectives, and ii) intractably large and highly complex search spaces (Zitzler et al., 2004). In extreme synthesis, the main properties of Evolutionary Algorithms (EAs) are that the search for the optima is conducted (i) using a (possibly) large population of multiple solution points or candidates, (ii) using operations inspired by the evolution of species, such as breeding and genetic mutation, (iii) using probabilistic operations and (iv) using information on the objective or search functions and not on its derivatives. The main advantages are: (i) fast convergence to near global optima, (ii) superior global searching capability in complicated search spaces and (iii) applicability even when gradient information is not readily achievable. MOEAs rely on the following concepts (Deb, 2001):

- Pareto front: The locus that is formed by a set of solutions that are equally good when compared to other solutions of that set is called Pareto front.
- Non-Domination: Non-dominated or Pareto-optimal solutions are those solutions in the set which do not dominate each other, i.e., neither of them is better than the other in all the objective function evaluations. The solutions on each Pareto front are Pareto-optimal with respect to each other.

The topology and capacity allocation optimization problems introduced before are both multi-objective in nature and present two conflicting objectives and complex search spaces: thus, they are suitable to be solved in the framework of MOEAs. The search space of the topology optimization problem is non-continuous, due to the binary nature of link connections: hence, the Non-dominated Sorting Binary Differential Evolution (NSBDE) algorithm (Li et al., 2013) is adopted for its solution. On the contrary, for the solution of the capacity allocation optimization problem, whose search space is continuous, a fast and elitist genetic algorithm, namely, NSGA-II (Deb et al., 2002), is applied.

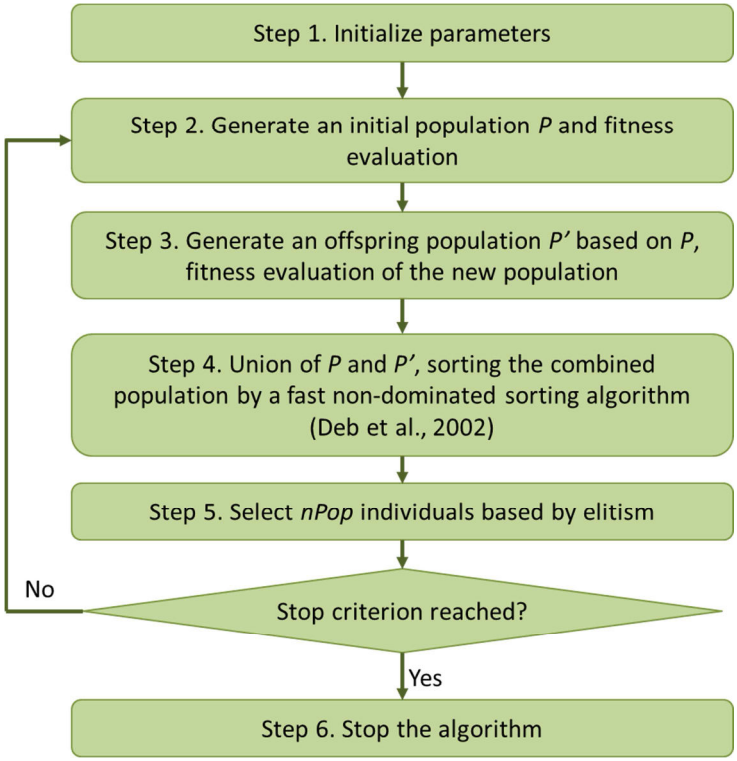


Figure 3:1 Flowchart of the common procedure of NSBDE and NSGA-II.

Figure 3:1 illustrates the common procedure of the two algorithms. It is only the way of generating new offspring (step 3) that differentiates the NSBDE from NSGA-II: in particular, the NSBDE algorithm replaces the crossover and mutation operators (typical of NSGA-II) using a variant of the modified binary differential evolution (MODE) (Wang et al., 2010). For details about the two algorithms, one can refer to appended Paper [3] and to Deb et al. (2002).

Chapter 4 Optimal restoration for enhanced CI resilience

While CIP has traditionally focused on physical protection and asset hardening (Bush, 2003; Lewis, 2006), lessons learned from recent catastrophic accidents have pushed part of the focus on the concept of "*resilience*"– i.e., the ability of an infrastructure network to rapidly *recover* from the effects of a disruptive event (Pursiainen, 2009; Obama, 2013). This chapter firstly addresses the issue of resilience definition and quantification for CI system. Section 4.2 proposes a framework for properly selecting recovery actions in order to optimize the resilience of infrastructure networks. Then, a heuristic dispatching rule is proposed to timely solve the resilience optimization problem in Section 4.3. Finally, two novel *resilience*-based component importance metrics (CIMs) are proposed in Section 4.4.

4.1 Definition of CI system resilience

4.1.1 Critical review of literature

Holling (1973) introduced the notion of *resilience* to the scientific world and provided the first system-level definition. Subsequently, the concept developed independently in disciplines ranging from environmental research to materials science and engineering, sociology, psychology and economics, giving rise to a number of different definitions and classifications of resilience within these fields (Henry and Emmanuel Ramirez-Marquez, 2012). Yet, it is believed that the current strong interest in resilience for infrastructure systems has been triggered in the aftermath of 9/11 attacks (Haimes et al., 2008).

One of the pioneering works in the field of infrastructure systems resilience is from the Multidisciplinary and National Center for Earthquake Engineering Research (MCEER) (Bruneau et al., 2003), where a general framework is provided to define and assess the seismic resilience of communities or any type of physical and organizational systems. This framework consists of "4Rs": robustness, redundancy, resourcefulness, and rapidity, while resilience itself encompasses four interrelated dimensions: technical, organizational, social and economic.

Based on the general framework provided by Bruneau et al. (2003), various studies have been carried out with the purpose of providing a practical interpretation of the concept of resilience and identifying possible ways of measuring it for giving support to resilience-based decisions. Most of these approaches to resilience interpretation and definition include aspects of a system withstanding disturbances, adapting to the disruption, and recovering from the state of reduced performance, and can rely upon a common concept which is illustrated schematically in Figure 4:1.

A quantifiable and time-dependent system performance function (also referred to system-level delivery function or figure-of-merit) $F(t)$ is the basis for the assessment of system resilience. It has a nominal value $F(t_0)$ under nominal operating conditions. The system operates at this level until suffering a disruptive event at time t_e. The disruption generally deteriorates system performance to some level $F(t_d)$ at time t_d. Then, recovery is started for increasing back system performance until a targeted level $F(t_r)$ is achieved once recovery is com-

pleted ($F(t_r)$ could be the same (as in Figure 4:1), lower or higher than the original system performance level $F(t_0)$). The dotted curve in Figure 4:1 denotes the targeted system performance $TF(t)$ if not affected by disruption. It is noted that various strategies exist for recovery activities, and system performance is ultimately a function of recovery decisions and actions. The period $t_d \leq t \leq t_r$ is generally considered as the recovery time (Cimellaro et al., 2010).

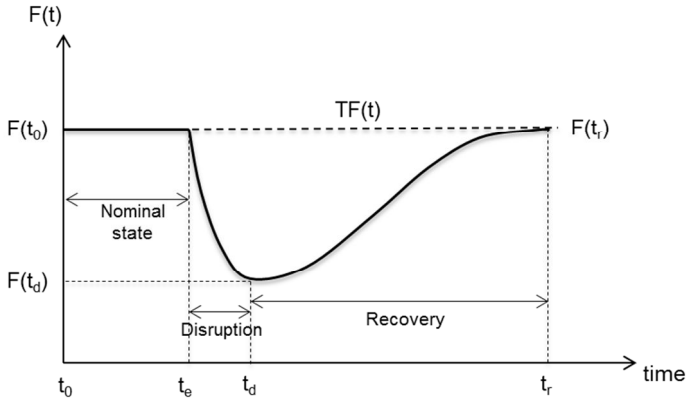


Figure 4:1 Generic system performance transition curve under the occurrence of a disruptive event.

Many studies in the literature define and measure resilience based only on initial system losses caused by disaster. Najjar and Gaudiot (1990) regard network resilience as a measure of network fault tolerance in a multicomputer system: in this framework, network resilience $NR(p)$ represents the upper bound on the number of node failures allowed, and is defined as the maximum number of node failures that can be sustained while the network remains connected with a probability $(1-p)$. Omer et al. (2009) suggest a model to measure resilience of a telecommunication cable system as a network infrastructure. The ratio of the "value delivery" of the network after a disruption to that before a disruption is defined as a reference for resilience, where "value delivery" is the amount of information that has to be carried through the network. Rosenkrantz et al. (2009) identify resilience metrics for service-oriented networks, where edge resilience of a network is defined as the largest value k such that, no matter which subset of k or fewer edges fail, the residual sub-network is self-sufficient. Node resilience is also defined in the same manner.

These definitions focus on the static "survival" property of a system, measuring the degree of system performance after a disruption. They largely overlap with the existing concepts of fault tolerance and robustness, while the temporal dimension of post-disaster loss recovery (i.e. the time $t > t_d$ in Figure 4:1) is not considered: on the other hand, this time period is significant for evaluating the system ability to leap back from disruption.

For this reason, other works have considered the system ability to recover from disruption. For example, MCEER (Bruneau et al., 2003) proposes that the seismic resilience of a community to an earthquake can be measured by the area between $F(t)$ and $F(t_0)$. Cimellaro et al. (2010) attempt to formulate a framework to quantify system resilience under seismic risk, taking into account both the losses due to the disaster and the recovery phase. They view system resilience as the area underneath the performance function $F(t)$ of a system, normalized by a control time t_{LC}. Ouyang and Dueñas-Osorio (2012) introduce a time-dependent resilience metric for infrastructure systems, where system resilience is quantified as the ratio of the area included between $F(t)$ and the time axis to the area included between $TF(t)$ and the time axis. The time span considered here is

from t_0 to a sufficiently large $t(t > t_r)$ that allows future system evolution: this metric explicitly embraces the system failure process.

Vulgrin et al. (2010) develop a composite resilience measure Z that simultaneously considers recovery of system performance and the resource expenditures required to achieve it. Two key quantities are computed: (i) the so-called systemic impact (SI) (defined as the cumulative impact of decreased system performance following a disruption and graphically represented by the area between the targeted system performance $TF(t)$ and the actual system performance $F(t)$) and (ii) the total recovery effort (TRE) (defined as the cumulative resources expended in recovery activities). However, the disadvantage of this approach is that an increase in SI and TRE implies an increase in its composite resilience measure Z ($Z = SI + \alpha\ TRE$), rather than a decrease.

Henry and Ramirez-Marquez (2012) attempt to review different definitions and metrics for system resilience, and introduce a resilience metric referring to the basic meaning of the word "resilience". They view resilience $R(t)$ as the ratio of recovery to loss at a given time t, measured by $R(t) = \frac{F(t)-F(t_d)}{F(t_0)-F(t_d)}$. This formulation is identical to Rose's (2007) static resilience metric when $F(t_d)$ is taken to be Rose's worst-case quantity. Henry and Ramirez-Marquez (2012), then, apply this measure to various scenarios that disable links in a transportation network in order to find restoration sequences that maximize recovery at a given time. However, this metric itself does not embrace the integral temporal dimension of the recovery process, thus neglecting the speed with which the performance of the system is recovered.

4.1.2 System resilience definition and assessment in this work

In light of the issues highlighted above, we propose a new metric for analytical quantification of the resilience of infrastructure systems. It is still relying on the basic meaning of the word "resilience" and can be applied to evaluate and compare the effectiveness of different strategies that are proposed to reduce adverse consequences of disruptive events.

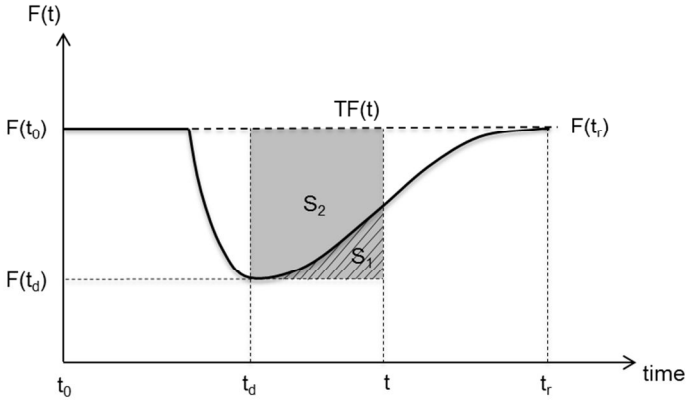


Figure 4:2 Conceptual illustration of the proposed resilience metric $R(t)$.

Let $R(t)$ be the resilience of a system at time t ($t \geq t_d$). In its basic form, $R(t)$ is here given the meaning of the cumulative system functionality that has been restored at time t, normalized by the expected cumulative system functionality during this same time period. Graphically, $R(t)$ is represented by the ratio of the area with diagonal stripes S_1 to the area of the shaded part S_2, as illustrated in Figure 4:2. Mathematically, it is given as:

$$R(t) = \frac{\int_{t_d}^{t}[F(\tau) - F(t_d)]d\tau}{\int_{t_d}^{t}[TF(\tau) - F(t_d)]d\tau}, t \geq t_d \tag{4.1}$$

The following considerations about the given resilience definition are important:

1) The system resilience $R(t)$ defined in Equation (4.1) measures the cumulative system performance that has been restored from the system disrupted state to the recovered state at current time t, normalized by the target cumulative performance as if the system were not affected by disruption. This formulation is aligned with the original meaning of the concept of resilience, while capturing at the same time both the magnitude and rapidity of the system recovery action.
2) The system performance function $F(t)$ could be represented by different metrics (e.g., the amount of flow or services delivered, the availability of critical facilities, the number of customers served, or the enabling potential of economic activities for infrastructure systems), depending on which dimension (i.e., technical, organizational, social and economic) of resilience the analysis focuses on (Bruneau et al., 2003). This study concentrates on the technical dimension of resilience and utilizes the amount of flow delivered to the demand nodes of a network as the performance level metric.
3) Note that $R(t)$ is undefined when $F(t_d) = TF(t)$, which means that a system does not suffer any loss. This condition is avoided since only systems exposed to disruptive events are here considered. Practically, if a system does not suffer any loss, there is no scope for it to be recovered or to bounce back and thus there is no need to evaluate resilience.
4) $R(t)$ is undefined when $t < t_d$, because of the same reason explained in item 3. Besides, this could avoid any overlap with existing concepts like robustness, vulnerability and survivability.
5) $R(t) \in [0, 1]$ and $R(t) = 0$ when $F(t) = F(t_d)$, which means that a system has not recovered from its disrupted state (i.e. there has been no "resilience" action); $R(t) = 1$ when $F(t) = TF(t)$, which corresponds to the ideal case where a system recovers to its target state immediately after disruption.
6) The target system performance $TF(t)$ is generally evolving due to the dynamic nature of service demand in infrastructure systems. For simplicity, in this study we assume that $TF(t)$ equals $F(t_0)$ and remains invariant.

4.2 Optimization model of CI system restoration

After the definition of system resilience, we focus on the role of various recovery decisions and actions in the task of optimizing the resilience of infrastructure networks subject to disruptive events. A general resilience optimization model for infrastructure networks is first formulated and, then, the DC power flow is incorporated as extra constraints when applying to power grids.

4.2.1 General flow-based modelling

The mathematical model for the resilience optimization problem here considered involves an infrastructure network $G(V, E)$ comprising a set of nodes V connected by a set of links E. The network nodes are classified into supply nodes V_S, transshipment nodes V_T, and demand nodes V_D ($V_S \cup V_T \cup V_D = V$). Each arc $ij \in E$ has an associated capacity $P_{ij} \in \mathbb{R}_0^+$, while each supply node $i \in V_S$ has a supply capacity per time unit $P_i^s \in \mathbb{R}_0^+$ and each demand node $j \in V_D$ has a demand $P_j^D \in \mathbb{R}_0^+$ per time unit. Network flow is sent from supply nodes to demand nodes respecting the flow capacities of the links and supply/demand capacities of the

nodes. Each unit of flow that arrives at demand node $j \in V_D$ is given a weight $w_j \in \mathbb{Z}^+$ in order to differentiate priorities of demand nodes (e.g., a hospital usually has a higher weight than a residential household in a power network). The performance of the network is evaluated by determining the maximum amount of weighed flow that can be received by the demand nodes. Formally, the system performance function is defined as:

$$F(t) = \sum_{j \in V_D} w_j f_j(t) \tag{4.2}$$

where $f_j(t)$ represents the amount of flow received by demand node j at time t.

Disruptions happen and create damages to nodes and/or links in the network, as modeled by the removal of a subset of arcs, $E' \subset E$.[1] The arcs in set E' are viewed as non-operational immediately after the disruption. System performance $F(t)$ achieve its minimum value at this time ($t = 0$, i.e. $F_{min} = F(0)$).

In a recovery optimization framework, we are not only interested in identifying a subset of the links in E' to be installed to the disrupted network, but also in selecting an optimal order of installation and repair of these links. The goal is to achieve maximum system resilience over the whole restoration horizon $T \in Z^+$. Link repairs are here assumed to be discrete tasks, and a repair cost $\beta_{ij} \in Z_0^+$ is associated to each arc $ij \in E'$. The processing time of a single arc restoration is not considered in this study (i.e., the repair action is assumed to be instantaneous); instead, the main focus is when the disrupted arcs should come back online. In addition, the number of arcs that can be restored in each time period is constrained by their total cost. By combining Equations (4.1) and (4.2), system resilience to be maximized at time T is given by

$$R(T) = \frac{\sum_{t=1}^{t=T} \left[\sum_{j \in V_D} w_j f_j(t) - F_{min}\right]}{T\left(\sum_{j \in V_D} w_j P_j^D - F_{min}\right)} \tag{4.3}$$

The optimization variables of the resilience optimization problem include: (i) continuous variables $f_{ij}(t) \in \mathbb{R}_0^+$, $ij \in E$ and $t = 1, \ldots, T$, that denote the flows moving from node i to node j through link ij at time unit t; (ii) continuous variables $f_j(t) \in R_0^+$, $j \in V_D$, that represent the amounts of flow received by demand node j at time unit t, and (iii) binary state variables $s_{ij}(t)$, $ij \in E$ and $t = 1, \ldots, T$, such that $s_{ij}(t) = 1$ if arc ij is operational and $s_{ij}(t) = 0$ if arc ij is not operational at time unit t.

We are interested in optimizing the resilience over the whole restoration process: thus, the timespan T is chosen as the total recovery time, defined as the period necessary to restore the system functionality to the same level as the original system. Consequently, the formulation of the resilience optimization problem is as follows:

$$\max \frac{\sum_{t=1}^{t=T} \left[\sum_{j \in V_D} w_j f_j(t) - F_{min}\right]}{T\left(\sum_{j \in V_D} w_j P_j^D - F_{min}\right)} \tag{4.4}$$

Subject to

[1] If nodes are important in a specific application problem, they can be converted to equivalent arcs by introducing additional arcs and nodes into the network, i.e. by 'splitting' a node into two nodes and an arc.

$$\sum_{ij\in E} f_{ij}(t) - \sum_{ji\in E} f_{ji}(t) \leq P_i^s, \forall i \in V_S, t = \{1, \dots, T\} \tag{4.5}$$

$$\sum_{ij\in E} f_{ij}(t) - \sum_{ji\in E} f_{ji}(t) = 0, \forall i \in V_T, t = \{1, \dots, T\} \tag{4.6}$$

$$\sum_{ij\in E} f_{ij}(t) - \sum_{ji\in E} f_{ji}(t) = -f_j(t), \forall i \in V_D, t = \{1, \dots, T\} \tag{4.7}$$

$$0 \leq f_j(t) \leq P_j^D, \forall i \in V_D, t = \{1, \dots, T\} \tag{4.8}$$

$$0 \leq f_{ij}(t) \leq s_{ij}(t) P_{ij}, \forall ij \in E, t = \{1, \dots, T\} \tag{4.9}$$

$$s_{ij}(t) \leq s_{ij}(t+1), \forall ij \in E, t = \{1, \dots, T\} \tag{4.10}$$

$$\sum_{ij\in E'} \beta_{ij}[s_{ij}(t) - s_{ij}(t-1)] \leq C(t), \forall t = \{1, \dots, T\} \tag{4.11}$$

$$s_{ij}(0) = 0, \forall ij \in E' \text{ and } s_{ij}(0) = 1, \forall ij \in E \backslash E' \tag{4.12}$$

$$s_{ij}(t) \in \{0,1\}, \forall ij \in E', t = \{1, \dots, T\} \tag{4.13}$$

The objective (4.4) is to maximize the system resilience over the time horizon of the problem. Constraints (4.5)-(4.9) are typical network flow constraints over the links and supply/demand nodes in the network in period t. They ensure that: (i) the flow generated at a supply node does not exceeds its supply capacity (4.5); (ii) the amount of net injected flow at a transshipment node is zero (4.6); (iii) the amount of net injected flow at a demand node is equal to the received flow at the node (4.7) while not exceeding its requested demand (4.8); (iv) the flow on an operational link does not exceed its capacity and there is no flow passing through an arc if the arc has not been repaired (4.9); constraint (4.10) ensures that once an arc has been restored at time t, it will keep operational thereafter; finally, constraint (4.11) ensures that the total cost paid for repairing links in a time period does not exceeds the available resources that can be allocated in this period.

4.2.2 Incorporating the DC power flow model for electrical networks

The general flow-based model introduced above assumes that we can directly control the flow in the network which is not the case for power infrastructure networks (see Bienstock and Mattia, 2007). The DC model is a commonly used linear approximation of the power grids to model its operations, especially the power transmission network (Purchala et al., 2005). The OPA cascading failure model (Dobson et al., 2001) is a typical example which based on the DC power flow model.

The DC model includes decision variables at each node of the network that represent the phase angle of the node. The flow on arc ij is then a function of the phase angles of nodes i and j along with the reactance of the arc ij. The reactance, b_{ij}, of the arc is dependent on the length of it and the voltage levels. By defining θ_i for $i \in N$ as the phase angle of node i, the flow on arc ij is determined by

$$b_{ij} f_{ij} = \theta_i - \theta_j \tag{4.14}$$

It is noted that both the phase angle variables and the arc flow variables are unrestricted in the DC model. A negative flow on arc ij corresponds to power flowing from node j to node i. Therefore, it is necessary to incorporate constraints that model Equation (4.14) into the optimization problem (4.4)-(4.13). To this end, we define variables $\theta_i(t)$ for $i \in N$ and $t = 1, \dots, T$ that represent the phase angle of node i in time period t. Then, the DC flow calculations (4.14) are enforced only when arc ij is operational at time t by using "Big-M" transformation (Coffrin et al., 2011), the constraints (4.9) will be replaced by:

$$b_{ij} f_{ij}(t) \leq \theta_i(t) - \theta_j(t) + M[1 - s_{ij}(t)], \forall ij \in E, t = \{1, \dots, T\} \tag{4.15}$$

$$b_{ij} f_{ij}(t) \geq \theta_i(t) - \theta_j(t) - M[1 - s_{ij}(t)], \forall ij \in E, t = \{1, \dots, T\} \tag{4.16}$$

$$-s_{ij}(t) P_{ij} \leq f_{ij}(t) \leq s_{ij}(t) P_{ij}, \forall ij \in E, t = \{1, \dots, T\} \tag{4.17}$$

If $s_{ij}(t) = 0$, then the constraint (4.17) force $f_{ij}(t) = 0$, while constraints (4.15) and (4.16) will not impose any restrictions on the relationship between the phase angles of nodes i and j due to the big M. If $s_{ij}(t) = 1$, then constraints (4.15) and (4.16) make sure that the DC flow Equation (4.14) is satisfied for arc ij in time period t while constraint (4.17) ensures that the capacity of the arc is not violated. The optimization problem (4.4)-(4.13) where constraints (4.9) has been replaced by constraints (4.15)–(4.17) will be applied to the restoration of power transmission networks.

4.3 A heuristic scheduling algorithm for optimization solution

The resilience optimization problem (ROP) introduced before is a mixed (binary) integer programming (MIP) problem, which has $O(|E| \cdot T + |V_D| \cdot T)$ continuous variables, $O(|E| \cdot T)$ binary variables and $O(|V| \cdot T + |E| \cdot T + 2|E'| \cdot T)$ constraints. It has been proven to be strongly NP-complete (Pinedo, 2012) and, thus, it is computationally intense especially for large-scale infrastructure networks composed of thousands of nodes and links.

It is noted that the evaluation of a potential solution to the ROP (i.e. of a scheduled set of recovery actions on the disrupted links) requires evaluating the state of the system at a given time, i.e. calculating the network flows, which is the result of a lower-level network flow optimization. This bi-level optimization structure differentiates the ROP from other resource-constrained project scheduling problems (RCPSP) extensively described in the literature (Brucker et al., 1999; Pinedo, 2012): these are generally based on the criterion of minimizing the makespan (the time to project completion) whose calculation is trivial. Consequently, many existing metaheuristic algorithms for RCPSP such as genetic algorithms (Hartmann, 1998), simulated annealing (Bouleimen and Lecocq, 2003), particle swarm (Jarboui et al., 2008) and ant colony optimization (Merkle et al., 2002) are most likely unable to solve the ROP without incurring in a large penalty in computational expense.

On the other hand, there has been a significant amount of studies in RCPSP proposing some so-called dispatching rules, which usually characterize the profitability of scheduling a certain task by evaluating its contribution to the objective function and then greedily schedule the unscheduled tasks with the best profitability (Pinedo, 2012).

The key point in designing a heuristic dispatching rule for our ROP is to understand how restoring an arc impacts the objective function Equation (4.3) of the problem. In this view, a straightforward idea is to modify the classical weighed shortest processing time (WSPT) first rule (Smith, 1956) by selecting the arc to be restored as

the one that maximizes the ratio of the improvement of system resilience and the cost of restoring the arc. However, this approach is short-sighted in the sense that some links will not enhance the system resilience (i.e. will not increase the amount of flow received by demand nodes) if they are not restored in a given predefined sequence with other transmission links. Thus, the profitability of restoring a *set* of arcs instead of a *single* arc is taken into account in designing our dispatching rule.

It is well known that the residual network associated with a maximum network flow does not contain an augmenting path from the supply node to the demand node (Ahuja et al., 1993). In this view, in order to increase the amount of flow received by the demand nodes in the current operational network after a disruptive event, a set of links forming some residual paths that have the potential to augment the flow received by the demand nodes must be restored. The main idea of our dispatching rule for the ROP is, then, to select a set of unrepaired links that belong to some residual path and that maximize the ratio of the potential augmented flow received by the demand nodes to the cumulative cost of repairing all the uninstalled links in this path. The potential augmented flow received by demand nodes is further limited by the following three elements: the residual capacity of the path, the residual capacity of the supply node and the unmet flow of the demand node.

Mathematically, suppose that $G_t(V, E_t)$ is a partially restored network at time t, X^* is the optimal flow (the result of the lower-level network flow optimization) associated with $G_t(V, E_t)$. The links in $G_t(V, E_t)$ will, then, have a residual capacity $RP_{ij} = P_{ij} - f_{ij}(t),\ \forall ij \in E_t$ and repair cost $\beta_{ij} = 0, \forall ij \in E_t$, since they are already operational. The supply and demand nodes in $G_t(V, E_t)$ will have a residual capacity $RP_i^s = P_i^s - f_i(t),\ \forall i \in V_S$ and unmet demand $RP_j^D = P_j^D - f_j(t),\ \forall j \in V_D$, respectively. The unrestored links in the disrupted link set E' have a residual capacity equivalent with their original capacity $RP_{ij} = P_{ij}$, and a repair cost β_{ij}. Then, the residual capacity of path $P_{s\to d}$ from supply node s to demand node d is defined as $R(P_{s\to d}) = min_{ij\in P_{s\to d}} RP_{ij}$. The cumulative cost of repairing all the uninstalled links in path $P_{s\to d}$ is $\sum_{ij\in P_{s\to d}} \beta_{ij}$. Then, we are interested in selecting the uninstalled links in the path to be repaired, that is an optimal solution to the following problem:

$$\max_{P_{s\to d}\in \aleph} \frac{min\{RP_s^S, RP_d^D, R(P_{s\to d})\} \cdot w_d}{\sum_{ij\in P_{s\to d}} \beta_{ij}} \tag{4.18}$$

where $\aleph$ is the set of all paths from all supply nodes to all demand nodes in the original network $G(V, E)$. The numerator of formula (4.18) provides a measure of the potential augmented (weighted) flow received at demand node d by restoring path $P_{s\to d}$ while the denominator measures the cost required to restore all disrupted links in path $P_{s\to d}$.

In order to determine an optimal path to (4.18), we suppose that $\gamma(P_{m\to n}) \cdot w_n$ is the numerator in an optimal solution to (4.18), i.e. $\gamma(P_{m\to n}) = min\ \ \{RP_m^S, RP_n^D, R(P_{m\to n})\}$; then, $P_{m\to n}$ is the path with the lowest cost in the network where we only include links whose residual capacities are greater than or equal to $\gamma(P_{m\to n})$. This leads to an algorithm to solve (4.18): for each potential value of the numerator (including each potential value of the residual capacity of a path, each residual capacity of supply nodes and each unmet flow of demand nodes), we determine the minimum cost path in the network comprising only these links whose residual capacities are larger than the numerator. The minimum cost path can be obtained by first constructing a weighed network, where the link weights are set as their repair costs and, then, searching the shortest path on the

weighed network constructed. We can, then, obtain an optimal solution in this procedure by marking the path that has the maximum value of ratio (4.18). It is noted that the residual capacity of a path is the minimum residual capacity of the links in the path, so there are at most $(|V_S| + |V_D| + |E|)$ different values to be considered, which means the next sets of links to be restored can be determined by solving $O(|V_S| + |V_D| + |E|)$ shortest path problems.

Table 4:1 Algorithm for path selection in the dispatching rule.

INPUT: Residual capacity RP_{ij} for each of the links $ij \in E$, residual capacity RP_i^s for each supply node $i \in V_S$, unmet demand RP_j^D and flow weight w_d for each demand node $j \in V_D$ in the current network $G_t(V, E_t)$ associated with an optimal flow X^*

Set $GlobalRatio = 0$, $P =$ null.

Sort the set $\{RP_{ij}\ RP_i^s\ RP_j^D\}$ in non-increasing order to obtain an ordered composite set R

for each $r \in \boldsymbol{R}$

  Construct a weighted network G^* including only the links, where $RP_{ij} \geq r$. The weight of a link is set as β_{ij} if it is a non-restored link; set the weight as 0 if it is an operational link

  for each $\boldsymbol{i} \in \boldsymbol{V_S}$ and $\boldsymbol{j} \in \boldsymbol{V_D}$

    Find the shortest weighed path $P^*_{i\to j}$ from i to j in the network G^*, calculate the path length $\boldsymbol{d}(\boldsymbol{P^*_{i\to j}}) = \sum_{(\boldsymbol{i},\boldsymbol{j})\in \boldsymbol{P^*_{i\to j}}} \boldsymbol{\beta}(\boldsymbol{i},\boldsymbol{j})$

    if $\frac{\min\ \{RP_i^S, RP_j^D, R(P^*_{i\to j})\}\cdot w_d}{d(P^*_{i\to j})} > GlobalRatio$

      $GlobalRatio = \frac{\min\ \{RP_i^S, RP_j^D, R(P^*_{i\to j})\}\cdot w_d}{d(P^*_{i\to j})}$

      $\boldsymbol{P} = \boldsymbol{P^*_{i\to j}}$

    end if

  end for

end for

Return $\boldsymbol{P}$

Formally, we provide the pseudo code of the algorithm for path selection in our dispatching rule in Table 4:1. We assume that the residual network $G_t(V, E_t)$ associated with an optimal flow X^* at a given time t has been calculated as part of the inputs of the algorithm. Other inputs include the residual capacity RP_{ij} for each link $ij \in E$, the residual capacity RP_i^s for each supply node $i \in V_S$, and the residual capacity RP_j^D and flow weight w_d for each demand node $j \in V_D$. The variable *GlobalRatio* flags the current optimal ratio in formula (4.18). The output of the algorithm is a path composed of the next set of arcs that should be restored to the network.

After obtaining the next set of links to be restored by applying the algorithm introduced above, we can easily allocate these link repair tasks into each timeslot subject to constraint (4.11), until all links from this set are restored. The link repair order within this set is not significant since we assume that a link repair task can be

split into two timeslots. Therefore, we can view this set of links as a queue and we will restore the next link in the queue once the previous task is finished. If no links are in the queue, we will determine the next set of links to be restored by considering the residual network associated with an optimal solution to the lower-level maximum flow problem, where all links that have been restored are regarded as operational in the network. This process continues until either all links are restored or the end of the time horizon is reached.

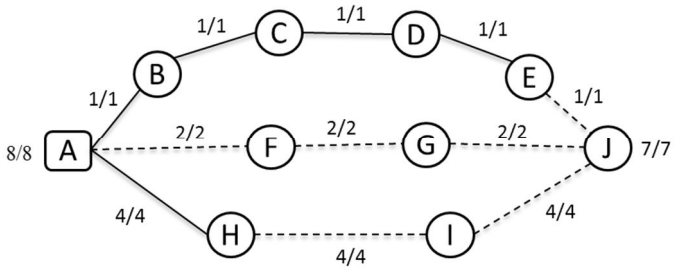


Figure 4:3 A simple disrupted network, where the dashed lines indicate failed arcs

We will illustrate the detailed steps of the above proposed algorithm by applying it to a very simple network. Consider the post-disaster network shown in Figure 4:3 with supply node A, demand node J and transship nodes B to I. The dashed lines in the figure indicate the failed arcs immediately after a disruptive event ($t = 0$), where the links *A-F*, *F-G*, *G-J*, *H-I*, *I-J*, *E-J* are disrupted. The numbers RP_{ij}/P_{ij} associated with each arc in the Figure represent the residual capacity RP_{ij} of the arc at time 0 and the original capacity P_{ij}. Note that the residual capacity of a failed arc is regarded as its original capacity, rather than zero. Similarly, the numbers 8/8 associated with the supply node A represent its residual capacity $RP_A^S = 8$ and its original capacity $P_A^S = 8$; the numbers 7/7 associated with the demand node J represent its unmet demand $RP_I^D = 7$ and flow demand $P_I^D = 7$, respectively. Besides, the repair costs of all the arcs are assumed to be constant and set as 1. The performance of the network is evaluated by the flow received by demand node J.

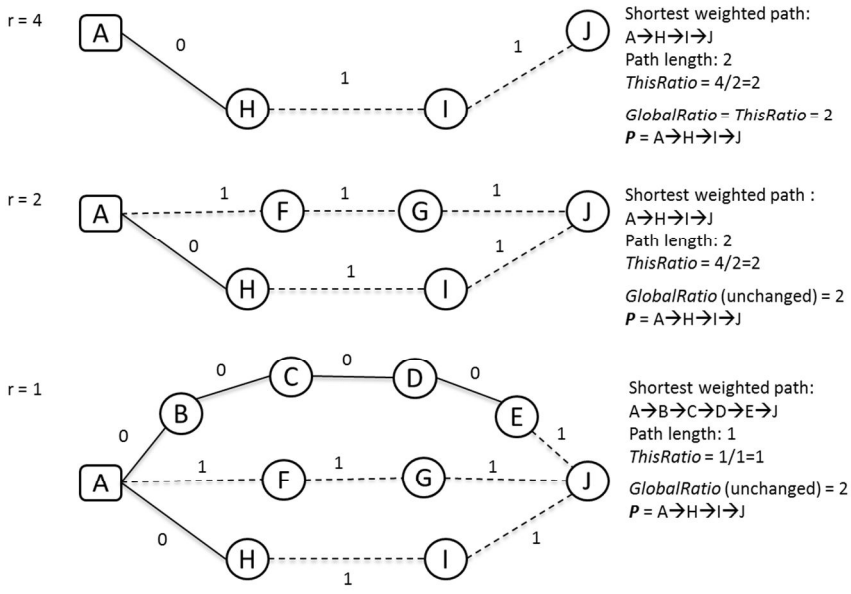


Figure 4:4 Illustration of the execution process of the path selection algorithm in Table 1 on a simple network.

The path selection algorithm in Table 4:1, first sorts the residual capacity array $\{RP_{ij}\ RP_i^s\ RP_j^D\}$ at current time ($t = 0$), resulting in a non-increasing set $R = \{8, 7, 4, 2, 1\}$; then, for each value in the set, the algorithm executes step 4 to step 11, illustrated graphically in Figure 4:4. Note that $r = 8$ and $r = 7$ are skipped since there is no weighed network associated to those two cases. The output of the execution $P = A \to H \to I \to J$ is the path that should be selected to be restored.

The network restoration is preceded by applying this path selection algorithm and then allocating these link repair tasks of the selected path into each timeslot subject to constraint (4.11). Assuming that only a single arc can be repaired at any given timeslot, we can obtain the optimal restoration curve of the network performance, as shown in Figure 4:5.

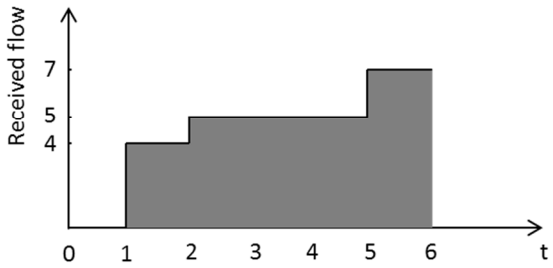


Figure 4:5 Optimal restoration curve of the network performance.

4.4 Resilience-based component importance measures (CIMs)

Based on the definition of system resilience and the resilience optimization framework, this Section addresses the issue of quantifying the *importance* of components in contributing to the *resilience* of a CI.

4.4.1 A brief overview

Various analytical and empirical CIMs have been proposed in the literature, e.g. Birnbaum (Birnbaum, 1968), Fussell-Vesely (Fussell, 1975), Reliability Achievement/Reduction Worth (Gandini, 1990; Levitin et al., 2003), and their extensions (Andrews and Beeson, 2003; Wang et al., 2014; Ramirez-Marquez and Coit, 2005, 2007), including those introduced in Chapter 2.3. CIMs have been shown valuable in establishing direction and prioritization of actions related to an upgrading effort (e.g., *reliability* improvement) in system design, or in suggesting the most efficient way to operate and maintain system status. However, none of the existing classical CIMs based on the reliability concept are directly applicable to the post-disaster phase, since there is no scope to exhibit reliability after the occurrence of system failure.

The role that a component plays in a network system has been measured by various so-called centrality measures, looking from the point of view of the complex interaction and communication flow in the network (Borgatti, 2005; Kröger and Zio, 2011). As already introduced in Chapter 2, classical topological centrality measures are the degree centrality (Nieminen, 1974; Freeman, 1979), the closeness centrality (Freeman, 1979), the betweenness centrality (Freeman, 1979), and the information centrality (Latora and Marchiori, 2007). They specifically rely on topological information to qualify the importance of a network component. Additionally, Freeman et al. (1991) proposed a *flow betweenness* centrality measure based on the idea of maximum network flow; Newman (2005) suggested a *random walk betweenness* measure that counts essentially all paths between

vertices and which makes no assumptions of optimality; Jenelius et al. (2006) proposed several vulnerability-based importance measures for transportation networks; Hines and Blumsack (2008) introduced an "electrical centrality" measure for electrical networks by taking into account the electrical topology of the network; Zio and Piccinelli (2010) provided a randomized flow model-based centrality measure specifically for electrical networks; Zio and Sansavini (2011a) introduced component criticality measures from the cascade failure process point of view, for general network systems. Nevertheless, none of these analyses takes into account the dynamics of system recovery from the effects of a disruptive event.

Resilience-based metrics of component criticality with respect to their influence on the overall resilience of the system (i.e., on the system's ability to quickly recover from a disruptive event) can be helpful for preparing an efficient component repair checklist in the event of system failure (Natvig et al., 2011). Recently, Baker et al. (2013) introduced two resilience-based network component importance metrics. However, the resilience definition, which the importance metrics rely on, does not embrace the temporal dimension of system recovery and it is, thus, unable to measure how fast the performance of a system comes back to an acceptable level. Besides, the two metrics do not quantify the influence that the recovery of particular components has on the overall resilience of the system and they are, thus, limited in providing valuable information for system restoration strategy making.

4.4.2 Resilience-based CIMs definition

The analysis concerns a network $G(V, E)$ comprising a set of nodes V and a set of links E. The binary state variable of arc ij at time t is denoted by $s_{ij}(t)$, $\forall ij \in E$. The initial impact experienced by the network after a disruptive event e at time $t = 0$ is represented by the removal of a subset of arcs, $E' \subset E$, from the network, setting $s_{ij}(0) = 0$, $\forall ij \in E'$. We introduce the failure probability of arc ij under event e, $p_e(ij)$

$$P[s_{ij}(0) = 0|e] = p_e(ij), \forall ij \in E \tag{4.19}$$

Equation (4.19) describes how individual components (links) are initially affected by a disruptive event e.

When considering component criticality in a resilience setting, we are interested in understanding: (i) the optimal time to repair the failed components in order to maximize system resilience, and (ii) the effect that the timely recovery of the components have on the overall resilience of the system. These concepts are at the basis of the definition of the two resilience-based importance measures here proposed.

Given a particular initial failure state, the optimal repair time (ORT) T_{ij}^{opt} of a failed arc ij can be computed by solving the MIP problem (4.4) - (4.13):

$$T_{ij}^{opt} = arg \max_{T_{ij} \in [0,T]} R(T) \tag{4.20}$$

The timespan for restoration, T, is chosen as the time period necessary to restore the system functionality to the same level as the original system. It is noted that the optimal repair time T_{ij}^{opt} offers an explicit quantification of the priority that should be given to the reparation and installation of arc ij into the network. Low values of T_{ij}^{opt} indicate higher priority of being repaired and re-installed into the network, i.e. higher ranking of the component in the repair checklist.

To account for the delay in the restoration of a particular link ij, a resilience reduction worth (RRW) metric is introduced as

$$RRW_{ij}(\Delta t_0) = \frac{R^{opt}(T) - R^{opt}(T|T_{ij} \geq T_{ij}^{opt} + \Delta t_0)}{R^{opt}(T)} \tag{4.21}$$

where $R^{opt}(T)$ represents the optimal system resilience at restoration time T; $R^{opt}(T|T_{ij} \geq T_{ij}^{opt} + \Delta t_0)$ corresponds to the optimal system resilience at time T if link ij cannot be repaired until time $(T_{ij}^{opt} + \Delta t_0)$, where Δt_0 is the delay with respect to its optimal repair time T_{ij}^{opt}, Equation (4.21) quantifies the potential (normalized) loss in optimal system resilience due to a delay Δt_0 in the repair of link ij. This metric is comparable to the so-called reliability reduction worth (Espiritu et al., 2007), which measures the potential damage caused to the system reliability by the failure of a particular component. It can provide valuable information to guide the recovery process of a particular component. Components with high values of $RRW_{ij}(\Delta t)$ should be given high priority in the restoration process, e.g. be assigned adequate restoration resources to avoid delays that would have a more significant impact on system restoration.

4.4.3 Methodology for component importance ordering

Ordering network links recovery on the basis of the values of the criticality measures described above, i.e., the optimal repair time T_{ij}^{opt} and resilience reduction worth RRW_{ij} (fixed Δt_0), requires quantifying the effect of timely repairing these links on the overall resilience of the system. Given the stochastic nature of disruptive events in terms of components failures after the event, the resilience-based criticality measures introduced are not represented by deterministic values, but rather by probability distributions. Therefore, given a network $G(V, E)$ under a disruptive event e, we first apply a Monte Carlo-based method to generate distributions of optimal repair time T_{ij}^{opt} and resilience reduction worth $RRW_{ij}(\Delta t_0)$ for all the links in the network; then, we rank links importance using a stochastic approach based on the Copeland's pairwise aggregation method (Merlin and Saari, 1997). The detailed steps of the algorithm are as follows:

Step 1. A network $G(V, E)$ is initially operating with a given parameters setting: flow demand P_j^D of all the demand nodes in V_D, supply capacity P_i^S of all the supply nodes in V_S and link capacity $P(ij)$ for all the network arcs in E.

Step 2. A failure configuration of the network is randomly sampled on the basis of the failure probabilities of each arc in the system given by Equation (4.19), under a disruptive event e at initial time $t = 0$. The operation state variables of failed links are set to 0, i.e., $s_{ij}(0) = 0$, $\forall ij \in E'$.

Step 3. The resilience optimization model of Equations (4.4) - (4.13) is applied and solved by Cplex to obtain the optimal strategy of network recovery, i.e., the optimal repair time T_{ij}^{opt} for each failed arc $ij \in E'$.

Step 4. In order to evaluate the second importance measure $RRW_{ij}(\Delta t_0)$, for each failed arc $ij \in E'$, the additional constraint that the restoration of arc ij should not be accomplished earlier than $T_{ij}^{opt} + \Delta t_0$ (i.e., $T_{ij} \geq T_{ij}^{opt} + \Delta t_0$) is added to the optimization model of Equations (4.4) - (4.13). Then, $R^{opt}(T|T_{ij} \geq T_{ij}^{opt} + \Delta t_0)$ is obtained by solving this "modified" optimization model by Cplex. Finally, the resilience reduction worth $RRW_{ij}(\Delta t_0)$ for each arc ij is recorded.

Step 5. To account for the stochasticity of the disruptive event in terms of arcs failures, repeat Step 2 to Step 4 for a chosen number $\aleph$ of iterations, generating probability distributions for T_{ij}^{opt} and $RRW_{ij}(\Delta t_0)$, for all the links in the network.

Step 6. Given the distributions of T_{ij}^{opt} (resp., $RRW_{ij}(\Delta t_0)$) for each arc ij, perform a stochastic ranking of links according to ascending (resp., descending) T_{ij}^{opt} values (see Section 4.4.4).

4.4.4 Stochastic ranking

In order to rank network links according to the distribution of their optimal repair time T_{ij}^{opt} (or resilience reduction worth $RRW_{ij}(\Delta t_0)$) obtained at step 6 of the algorithm above, an approach based on the Copeland's pairwise aggregation method (Merlin and Saari, 1997) is proposed. The Copeland's method (CM) is a simple non-parametric Condorcet method used in the political field (voting) that does not require any information about decision maker preference and operates on a multi-indicator matrix formed by m objects characterized by Ω attributes (Pomerol and Barba-Romero, 2000). CM relies on pair-wise comparisons between objects in the candidate pool, and the so-called Copeland score is defined for each object as the difference between the number of times that this object beats the other objects and the number of times that it is beat by other objects.

The CM-based ranking approach applied here corresponds to a modification proposed by Al-Sharrah (2010). It first examines the CDF of a given variable for all the candidates, e.g., the CDF of $T_{ij}^{opt}, \forall (i,j) \in E$; then, it compares the CDF of two candidates under analysis, i.e., links ij and $\overline{ij}$, with respect to specific attributes q_k of the CDF: for example, attribute q_k may represent the kth percentile. Subsequently, a quantity $S_k(ij, \overline{ij})$ is calculated based on a pairwise comparison between links ij and $\overline{ij}$ with respect to (percentile) q_k of the corresponding distributions, $k = 1, \ldots, \Omega$:

$$S_k(ij,\overline{ij}) = \begin{cases} C_{k-1}(ij,\overline{ij}) + 1, & \text{if } q_k(ij) \text{ beats } q_k(\overline{ij}) \\ C_{k-1}(ij,\overline{ij}) + 0.5, & \text{if } q_k(ij) \text{ and } q_k(\overline{ij}) \text{ are tied} \\ C_{k-1}(ij,\overline{ij}), & \text{if } q_k(ij) \text{ beats } q_k(\overline{ij}) \end{cases} \tag{4.22}$$

where the sentence "$q_k(ij)$ beats $q_k(\overline{ij})$" means that $q_k(ij)$ dominates $q_k(\overline{ij})$ with respect to the ranking rule of the variable considered, i.e., $q_k(ij) < q_k(\overline{ij})$ for T_{ij}^{opt}, while $q_k(ij) > q_k(\overline{ij})$ if $RRW_{ij}(\Delta t_0)$ is considered. $S_0(ij, \overline{ij})$ is initialized at zero for the first (percentile) q_1 and Equation (4.22) is iterated through all Ω attributes (percentiles). Then, the Copeland score for each link ij is defined as

$$C(ij) = \sum_{\overline{ij} \neq ij} S_\Omega(ij, \overline{ij}) \tag{4.23}$$

This Copeland score is finally used to rank all the links: the higher $C(ij)$, the higher the contribution of link ij to the overall resilience of the network.

Chapter 5 Applications

This Chapter reports the results of the application of the models and methodologies described in the previous Chapters to realistic CI networks. Only main results and insights are provided, while for further details the interested reader is referred to the corresponding Papers [1-6] of Part II.

5.1 Applications of the hierarchical network representation framework

It is known that most network reliability problems are NP-hard and therefore there is a significant gap between theoretical analysis and the ability to compute different reliability parameters for large or even moderately large network systems (Gertsbakh and Shpungin, 2008). In this respect, the hierarchical network representation proposed in Chapter 2 sets up a framework in which the reliability and vulnerability characteristics of complex network systems can be computed efficiently, due to the multi-scaled information representation scheme.

In this Section, we refer to a realistic CI network, i.e. the 380kV Italian Power Transmission Network (IPTN380) (see Figure 5:1), to illustrate how the hierarchical representation framework can be applied to the analyses of network (node-pair) reliability and to the computations of the extended CIMs.

Figure 5:1 The 380kV Italian Power Transmission Network (IPTN380) (Zio and Sansavini, 2011a).

The IPTN380 (Figure 5:1) is a branch of the high-voltage-level transmission, which can be modeled as a graph of $N = 127$ nodes connected by $M = 171$ links. It is important to underline that only the topology of the physical system is taken as reference and used in the analyses, so that the hierarchical model and clustering relate only on the network structure with no specific relation to the electrical properties of the system.

The network has been modeled as a five levels hierarchy (to which correspond five fictitious networks) by successively applying the USCA introduced in Chapter 2.2.1. Figure 5:2 presents the hierarchy structure of the IPTN380 and the artificial networks associated with the first 3 levels of the hierarchy. At the top of the hierarchy (i.e. $l = 1$), the network is a single unit, i.e. one artificial vertex $V_1^{(1)}$, which consist of all actual nodes. At the second level, we have $\Lambda^{(2)} = \left\{V_1^{(2)}, V_2^{(2)}, V_3^{(2)}, V_4^{(2)}\right\}$ and $E^{(2)} = \left\{E_{13}^{(2)}, E_{14}^{(2)}, E_{34}^{(2)}, E_{24}^{(2)}\right\}$ with

$V_1^{(2)}, V_2^{(2)}, V_3^{(2)}, V_4^{(2)} \subset V_1^{(1)}$. The integer number indicated in Figure 5:2 in proximity of the generic i-th artificial node $V_i^{(2)}$ indicates the number of actual nodes which compose it: e.g. $V_1^{(2)}$ is representative of a group of 38 actual network nodes. Note that at the bottom of the hierarchy, we find the original network, i.e. each artificial node is an actual node and each artificial edge corresponds to an actual link.

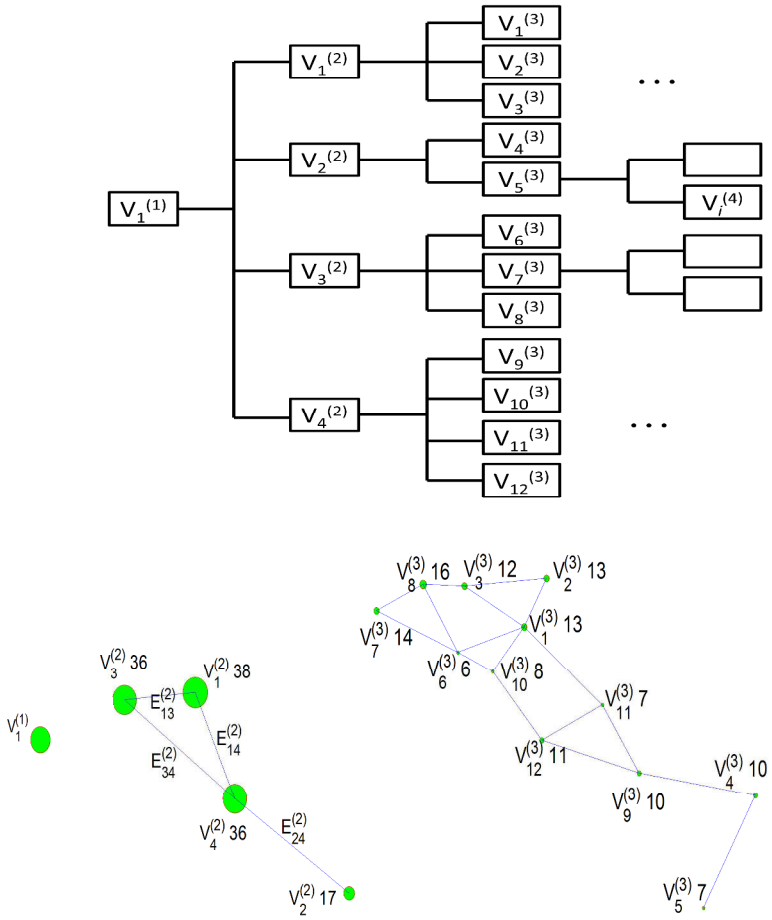


Figure 5:2 The hierarchy structure of the IPTN380 and associated artificial networks of the first three levels.

5.1.1 Terminal pair reliability analysis

The terminal-pair or node-pair reliability (TPR) problem amounts to determining the probability of successful communication between a specified source node and a terminal node in a network, given the probability of success of each link and node in the network. When the computational cost of the network is high (it grows exponentially with the number of network components), then the artificial network at a suitable level of the hierarchy can be leveraged to carry out the analysis of TPR. For a detailed interpretation of TPR based on the hierarchical framework, one can refer to appended Paper [2].

In Figure 5:3 right-panel, the connection reliability between nodes 1 and 127 in the IPTN380 (left panel in Figure 5:3) is shown as resulting from evaluations at each of the five levels of the hierarchical model described in the previous Section. The right panel of Figure 5:3 gives the probabilities of connectivity failure between nodes 1 and 127 from level 2 to level 5 (top) and the computational time needed for the analysis (bottom); the values have been normalized with respect to the maximum values of connectivity failure probability and computational time, which occur at the bottom of the hierarchy (level 5) corresponding to the whole network. The

result at the first level has not been shown since its value is simply 0, i.e., node 1 and 127 are in a single unit and will not disconnect. One can see that the difference between the actual and estimated failure probabilities decreases as the assessment moves downs to the bottom of the hierarchy, balanced by the computation time which instead increases significantly. The decision maker can obtain satisfying estimations of the failure probability at a hierarchical level of lower complexity, e.g. level 3, thus saving significant computation time.

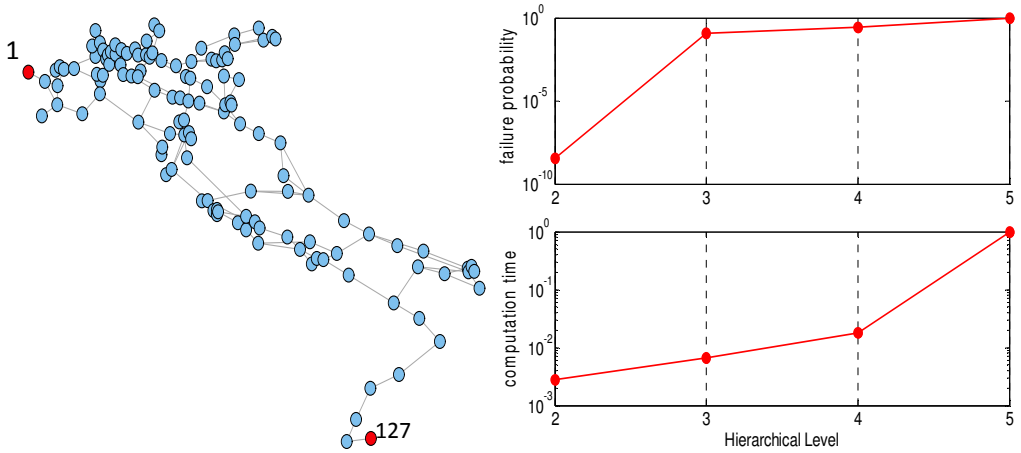


Figure 5:3 Illustrative example of terminal pair reliability assessment of IPTN380.

5.1.2 Computation of the extended CIMs

In Chapter 2.3, three extended CIMs, i.e. EBI, ECI and EFVI, have been introduced to account for the multiple terminal or node pairs (e.g. generator-distributor pairs) of a network system where connectivity defines the network functionality.

The extended CIMs introduced have been calculated for the IPTN380 at different levels of the hierarchical model of the system developed. For the evaluation, an artificial node functions as a generator as long as there is at least one actual generator node within it; otherwise, it is simply a distributor.

Table 5:1 EBI and EFVI at level 2 of the hierarchical model.

Artificial Edge	EBI		EFVI		Associated Actual Edges
	Rank	Value	Rank	Value	
{2-4}	1	0.3750	1	0.3750	{107-109,112-114,110-111}
{1-4}	2	1.9606E-03	2	1.9605E-03	{64-78,71-83}
{1-3}	3	1.4817E-03	3	1.4817E-03	{59-60,61-62,30-34,30-31}
{3-4}	4	1.5100E-05	4	1.4900E-05	{76-79}

Table 5:2 ECI at level 2 of the hierarchical model.

Artificial Edges	Rank	ECI	Associated Actual Edges
{2-4}	4	0.37	{107-109,112-114,110-111}
{1-4}	2	7699812.62	{64-78,71-83}
{1-3}	3	16.55	{59-60,61-62,30-34,30-31}
{3-4}	1	7699828.67	{76-79}

Table 5:1 and Table 5:2 report the results of the importance assessment (EBI, EFVI are given in Table 5:1 and ECI in Table 5:2) for the artificial edges of the network at level 2 of the hierarchy. For EBI and EFVI, all components in the artificial network have the same importance rank, but with slight differences between EBI and EFVI values; also the artificial edge {2-4} is the most important in the artificial network (see the bottom panel of Figure 5:2). This is due to the fact that this artificial edge is the only possible link between a generator in artificial node $V_2^{(2)}$ and the distributors in other artificial nodes, and thus its disconnection would cause a large-scale generator-distributor connectivity failure. The rank based on the ECI is different from that of EBI and EFVI, and the most important artificial edge is {3-4}; the difference lies in the definition, as discussed before: EBI depends only on the structure of the system and not on the reliability of the considered component, whereas ECI takes the unreliability of the component into consideration; in fact, the artificial edge {3-4} is made of only one actual edge with relatively high probability of failure, which leads to the highest ECI value.

By combining the indications of EBI and ECI, it is advisable to offer indicators to the decision maker for the purpose of system maintenance and operation optimization (Van der Borst and Schoonakker, 2001). When EBI & EFVI is high and ECI is low, like in the case of artificial edge {2-4}, system safety can be improved by protecting against failure of each component, e.g., by adding alternative edges between artificial node $V_2^{(2)}$ and node $V_1^{(2)}$ (or $V_3^{(2)}$). For the case of low EBI & EFVI and high ECI (artificial edge {3-4}), the decision maker should invest in improvements of the component itself, to decrease the failure probability.

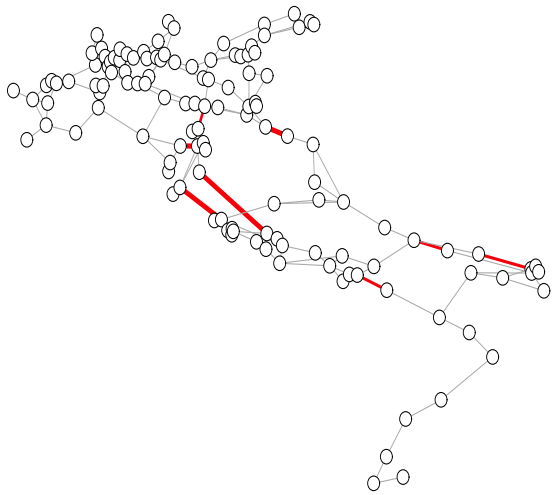


Figure 5:4 Most critical edges at level 3 of the hierarchical model.

Table 5:3 EIMs evaluation time at each level of the hierarchical model.

EIMs	Computation time (seconds on a computer with 2 CPU 3.06G 3.07G)		
	Level 2	Level 3	Level 4
EBI	0.3856	108.5	31763.58
EFVI	0.2086	112.2	32179.50
ECI	0.5152	175.0	47621.58

For details about the results of the EIMs at levels 3 and 4 of the IPTN hierarchical model, one can refer to the appended Paper [2]. Interestingly, the bold edges in Figure 5:4 represent the edges of the actual network system which have resulted most critical based on the extended importance measure evaluation carried out at level 3 of

the hierarchy model. These edges should be paid special attention. For links {110-111, 112-114, 107-109}, improving the defense in depth against their failures is advisable for improving the reliability of the system, whereas for links {64-78, 71-83, 76-79, 80-95, 75-88}, the edge unreliability should also be mitigated.

More importantly, Table 5:3 reports the computation times required for the calculations of the EIMs at different levels in the hierarchy: as expected, the more we go down in the hierarchy, the higher the computation time.

5.1.3 Brief summary

The introduced framework for hierarchical modelling of large-scale CI network systems, which leads to the definition of different varied-size grained artificial networks, provides a multi-scaled representation of the system, with more detailed information but high complexity at the lower levels of the hierarchy, and simplified structure, but relatively low complexity at the higher levels. The availability of different scales of modeling resolution allows a flexible management of the analysis, at the level of details desired for its purposes. The computations of network node-pair reliability and the extended CIMs involving the IPTN380 have demonstrated the effectiveness of the proposed method.

5.2 Network optimization against cascading failures – comparative study

Figure 5:5 The 400kV French power transmission network (FPTN400) (RTE, 2011).

This Section applies the frameworks of network optimization against cascading failures proposed in Chapter 3 to the 400kV French Power Transmission Network (FPTN400) (see Figure 5:5). This network has 171 nodes (substations) and 220 edges (transmission lines). We distinguish the generators, which are the source of power, from the other distribution substations, that receive power and transmit it to other substations or distribute it in local distribution grids. By obtaining the power plants list from EDF website (EDF, 2013) and relating them with the ID of the buses in the transmission network, we have 26 generators and 145 distributors. Only the nuclear power plants, hydroelectric plants and thermal power plants whose installed capacities are larger than 1000 MW, are considered.

5.2.1 Topology optimization based on the ML model and its validation by the OPA model

For the optimal reallocation of the power generating nodes to the other nodes of the FPTN400 (i.e., the topology optimization proposed in Chapter 3.3.1), we utilize the NSBDE algorithm detailed in appended Paper [3].

The Pareto front obtained by the NSBDE algorithm at convergence is illustrated in Figure 5:6, where the diamond point represents the current network with the present pattern of connecting links, which is also the least costly network; the square point is the most resilient network, whose cascading vulnerability is 0.184. It is not unexpected that the original network is the least costly one, since the electrical transmission lines and substations are placed with geographical constraints and connections between two distant substations are avoided. Actually, cost-effectiveness is a major consideration in constructing real power transmission networks.

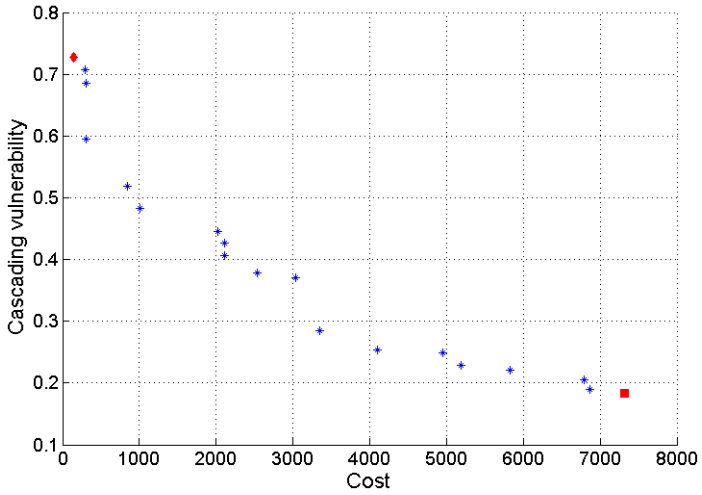


Figure 5:6 Pareto front reached by a population of 25 chromosomes evolving for 300 generations.

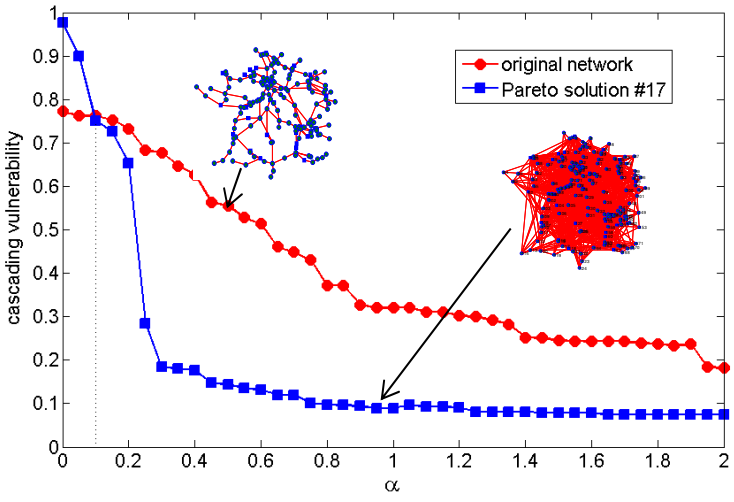


Figure 5:7 Comparison of the cascading vulnerability between the original and the most resilient networks under different network tolerance values.

It is also noted from Figure 5:6 that the cascading failure resilience of the FPTN400 can be improved significantly by properly rewiring the generator-distributor connections, though at a cost; the network vulnerability is decreased from 0.728 to 0.184 (when the tolerance parameter α=1.3) with an increased cost of 7.3×10^3 (i.e., 53.16 times increase). Figure 5:7 reports the cascading vulnerability comparison between the original network

and the most resilient one (Pareto solution #17) with different values of the tolerance parameters α. It shows that when the network tolerance is very low, i.e. $0 < \alpha < 0.1$, the optimized network loses most of its efficiency, i.e., it is quite vulnerable to intentional attacks, possibly due to its intensive loading condition. However, when $\alpha \geq 0.3$ (which is generally the normal operating condition (Baldick et al., 2008)), the optimized network loses less than 20% of its efficiency during a cascading failure initiated by intentional attack.

Albeit a substantial improvement of the cascading failure resilience of the FPTN400 is possible by adding redundant links, a tradeoff between the cost and resilience improvement is necessary for rational decision-making. Along the Pareto frontier of the potential solutions, there are some points at which a small sacrifice of cost gives a large gain of cascading resilience. More generally, by taking a network solution and its neighbor on the frontier (the less costly one), one can define a rate of change of cascading resilience with respect to cost: $|\Delta Vul/\Delta cost|$. This rate can be utilized as a reference to choose the optimized network: the larger the ratio, the more preferred the network is.

The optimization results presented above are based on the ML model which abstracts basic power flow constraints and electrical characteristics of the power transmission network. Thus, the more realistic OPA model is, then, utilized to validate a posteriori the optimal results found. The verification is not straightforward due to the differences of the two models in the way of representing and initializing system capacity, in the iterative algorithms they rely on, and in the way of measuring the damage produced by the cascading failure. Accordingly, some assumptions and adjustments to the OPA model (see appended Paper [3] for the details) have been taken to ensure its applicability to assess the optimization solutions obtained based on the ML model.

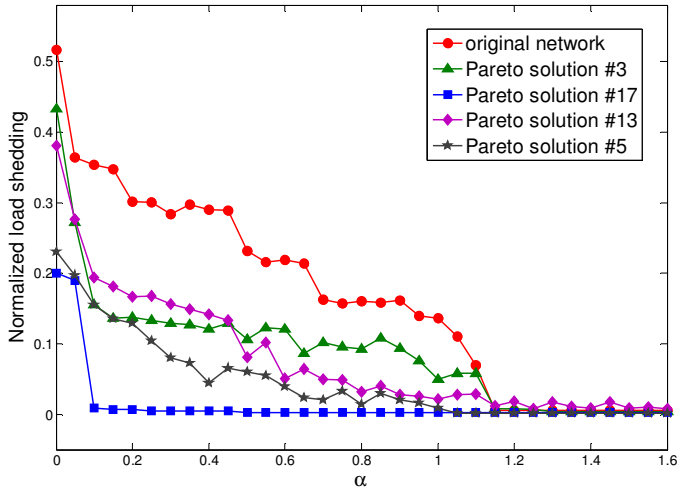


Figure 5:8 Cascading vulnerability (normalized load shedding) evaluated by the OPA model for the five chosen networks over a range of network tolerance values α under targeted initial failure.

Five representative solutions (i.e., the least cost network FPTN400, Pareto solution #17 (7300, 0.184) which is the most resilient, together with solutions #3 (310.6, 0.59), #5 (3344.3, 0.28) and #13 (1003.8, 0.48) whose $|\Delta Vul/\Delta cost|$ values are comparatively large) along the Pareto front in Figure 5.6 are chosen as the basic network topologies to be verified by the OPA model.

In Figure 5:8, we plot the curves of normalized load shedding LS/D (Equation 3.11) versus network tolerance α obtained by applying the OPA model to the five representative networks selected from the Pareto front (obtained using the ML model). The OPA simulation is triggered by removing one of the top five most loaded

nodes (i.e., by a targeted initial failure). Analogous to the ML model (Figure 5:7), the network damages decreases when network tolerance increases for all the networks. When network tolerance value is high enough ($\alpha > 1.2$), any small intentional disturbance on the network would tend to cause quite low damage to the functioning of the network ($< 1\%$). Most importantly, it is observed that in the OPA simulation, the network corresponding to Pareto solution #3 (310.6, 0.59) (green triangle curve) is more resilient, i.e., it presents less load shedding than the original network (red circle curve) over a wide range of network tolerance α (i.e., $0 < \alpha < 1.2$); in addition, solution #13 (1003.8, 0.48) (magenta diamond curve) generally outperforms solution #3, while solution #5 (3344.3, 0.28) (grey star curve) outperforms #13 in terms of cascade resilience. Finally, Pareto solution #17 (7300, 0.184) (which is the most resilient network according to the ML model) presents the lowest load shedding among the five networks over the entire range of α values considered. This ranking of cascading failure resilience in the OPA model is consistent with the simulation results based on ML model.

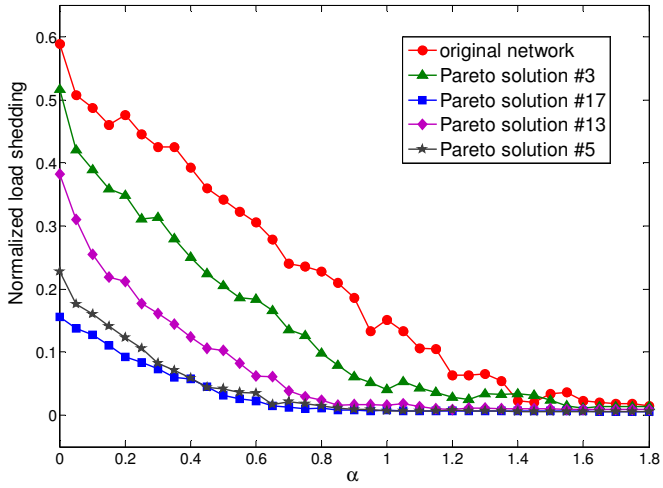


Figure 5:9 Cascading vulnerability (normalized load shedding) evaluated by the OPA model for the five chosen networks over a range of network tolerance values α under random initial failure. The results have been averaged over 30 different samples.

Figure 5:9 shows the results of OPA simulation on the five networks, where the failures are triggered by removing a randomly chosen node (i.e., random initial failure) and the results are averaged over 30 different samples. The ranking of cascade resilience of the five networks here is also parallel with the optimization results based on ML. This demonstrates that a resilience-improved network from the optimization based on the ML model is also more resilient than another one if evaluated by the more realistic OPA cascade simulation, therefore, verifying that the insights gained by the topological optimization approach are valid.

It is also important to remember that the results produced by the simple ML topological model are obtained at a much lower computational cost than those of the OPA model: actually, the average time needed to carry out a single cascading failure simulation is 3.9s and 20.8s for the ML and OPA models, respectively, on a double 2.4 GHz Intel CPU and 4 GB RAM computer.

5.2.2 Capacity allocation optimization based on the ML and OPA models

For optimal allocation of link capacity in the FPTN400 network, the NSGA-II algorithm is applied with regards to the objectives of minimizing investment cost and cascade vulnerability, expressed by functions (3.12a) and (3.12b), respectively, in Chapter 3. Differently from the previous Section 5.2.1, both the ML and OPA

models are used directly in the optimization process to evaluate the cascade vulnerability of the proposed network. It is evident that the ML and OPA models provide different results at the local scale (Cupac et al., 2013); however, in this study we evaluate to what extent the two approaches are consistent at the global system level. In particular, we compare the two approaches by performing the following analyses:

- We verify whether the Pareto fronts based on the ML and OPA models exhibit similar characteristics in terms of phase transitions of cascade vulnerability with respect to normalized investment cost;
- We investigate whether the Pareto optimal solutions showing the same level of investment cost also present similar capacity allocation patterns;
- We examine whether the link capacities patterns along the two optimal frontiers exhibit similar characteristics for decreasing network vulnerability (i.e. for increasing network resilience).

Figure 5:10 shows that ML and OPA Pareto fronts exhibit similar phase transitions (although their absolute values are different, which is not unexpected considering the fact that they apply different modelling parameters and cascade vulnerability measures): both curves present a sharp decrease in network vulnerability in the same $\overline{Cost}$ region (i.e. $1.0 \leq \overline{Cost} \leq 1.5$), where a small increase in the cost gives a large gain in terms of cascade resilience. Besides, regions of plateau exist for certain cost values in both models (i.e. for $1.5 \leq \overline{Cost} \leq 1.75$ and $2.0 \leq \overline{Cost} \leq 2.2$ in ML, and for $1.5 \leq \overline{Cost} \leq 1.8$ and $2.15 \leq \overline{Cost} \leq 2.45$ in OPA), in which increasing investment cost does not improve network resilience. Finally, both curves show a relatively stable regime for large $\overline{Cost}$ values (i.e., $\overline{Cost} \geq 2.2$), where network resilience is already high and its relative improvement is negligible even for a significant increase in the network cost (for example, referring to the ML model, increasing $\overline{Cost}$ from 1.97 to 2.61, i.e., of 32.5%, we reduce the network vulnerability of only 1.5%).

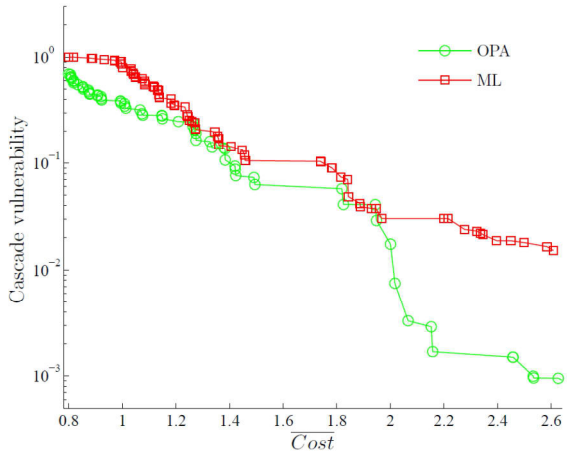


Figure 5:10 Phase transitions in the Pareto optimal fronts showing cascade vulnerability (i.e., average efficiency loss for ML and average load shedding for OPA) with respect to normalized investment cost.

Then, we compare the link capacities patterns of those solutions along the two Pareto fronts that present approximately the same values of $\overline{Cost}$. In particular, three representative values of normalized cost (i.e., $\overline{Cost}$=1.07, 1.27 and 1.81) along the Pareto fronts are chosen, and the relationship between the link capacities of the corresponding optimal solutions obtained by the ML and OPA models are visualized using the scatterplots of Figure 5:11(a), (b) and (c), respectively. It is evident that the link capacities of the optimal solutions based on the ML and OPA models are highly correlated (with correlation coefficient $r_{ML,OPA}$=0.73, 0.69 and 0.76, respectively). That is, links with low capacity in the ML model are likely to have low capacity also in the OPA model, and links with high capacity in ML also have high capacity in OPA.

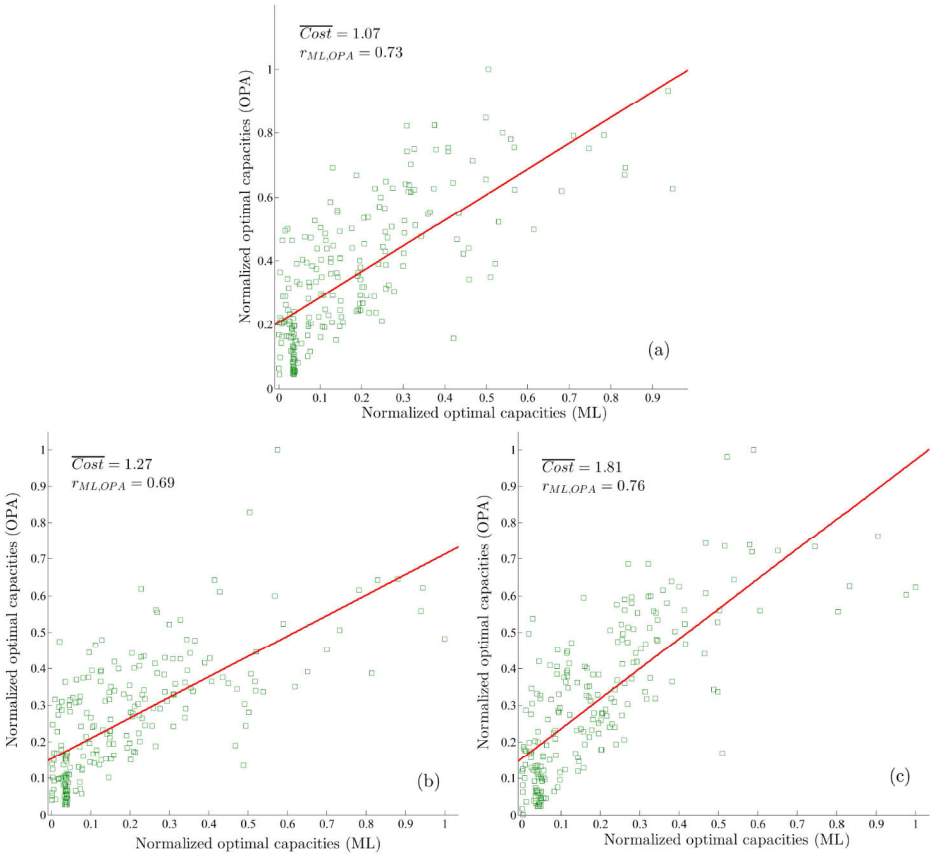


Figure 5:11 Scatter plot of the (normalized) link capacities of three representative ML and OPA Pareto solutions showing the same normalized cost. The link capacities of the Pareto solutions with the same level of cost show highly correlated allocation patterns: (a) ML solution (1.07, 0.63) versus OPA solution (1.07, 0.30): $r_{ML,OPA} = 0.73$; (b) ML solution (1.27, 0.24) versus OPA solution (1.27, 0.21): $r_{ML,OPA} = 0.69$; (c) ML solution (1.81, 0.074) versus OPA solution (1.81, 0.057): $r_{ML,OPA} = 0.76$. The line of best fit is also plotted, for visual guidance.

Finally, it is interesting to analyse how the pattern of link capacities changes when lower network cascade vulnerability (higher network resilience) is demanded, i.e., which type of capacity allocation pattern is the most favourable in resisting to cascading failures. We tackle this problem by investigating the "expected" network link capacity pattern as a function of cascade vulnerability, i.e., the configuration of capacity pattern "averaged" over all possible solutions of the Pareto front lying within a given "regime" (i.e., interval) of cascade vulnerability of interest. Parameter β^s (namely, β^s_{ML} for ML and β^s_{OPA} for OPA) is used to represent the "regime" of vulnerability, where s indicates the size of the corresponding interval. It is noted that smaller β^s represents higher network resilience.

Figure 5:12 reports the results of averaged link capacities patterns for three different levels of cascade vulnerability, i.e., $0.6 \leq \beta^{0.1} \leq 0.7$, $0.3 \leq \beta^{0.1} \leq 0.4$ and $0 \leq \beta^{0.1} \leq 0.1$ in the case of a classical homogeneous allocation strategy (circles) and of the optimization-based approach of our study (squares). The left panel (a-c) is referred to ML, whereas the right panel (d-f) relates to OPA. It is found that the optimal link capacity patterns exhibit consistent characteristics between ML and OPA models. For example, in both cases, the optimal link capacities patterns are similar to their corresponding homogeneous allocations only in less resilient networks, i.e., when $0.6 \leq \beta^{0.1} \leq 0.7$, where the objective of minimizing investment cost is much more biased (Figure 5:12(a) and (d)). When we increase the importance of minimizing the network vulnerability (e.g., for

$0.3 \leq \beta^{0.1} \leq 0.4$ and $0 \leq \beta^{0.1} \leq 0.1$), the optimal link capacities show a non-linear relationship with respect to their initial flows, as shown in Figure 5:12(b), (c) and Figure 5:12(e), (f). Specifically, the heavily loaded links tend to decrease their capacities and the lightly loaded links tend to increase their capacities. That is to say, the unoccupied portion of capacity tends to decrease in links with larger loads and the unoccupied portion of capacity tends to increase in the less loaded links. Furthermore, the more importance is given to the minimization of network cascade vulnerability, the more pronounced the non-linear behaviour is, as shown in Figure 5:12(c) and (f). Our findings are consistent with the empirical observations and results from the traffic fluctuation model (Kim and Motter, 2008a; 2008b).

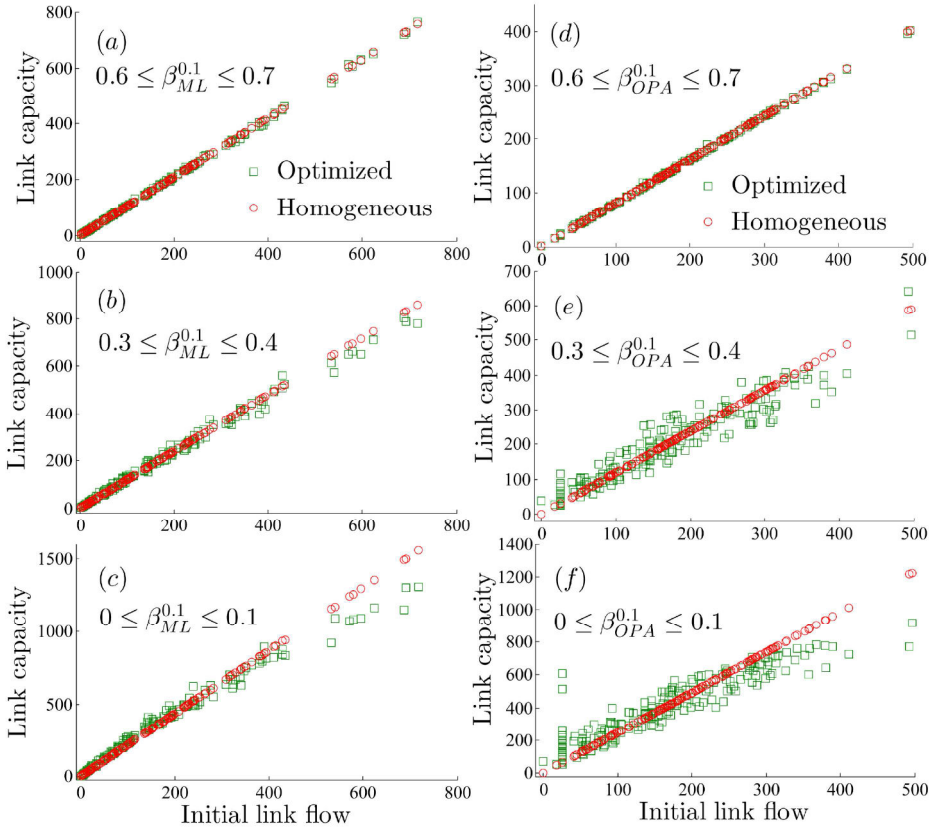


Figure 5:12 "Averaged" optimal link capacity patterns for three different levels of cascade vulnerability ($0.6 \leq \beta^{0.1} \leq 0.7$, $0.3 \leq \beta^{0.1} \leq 0.4$ and $0 \leq \beta^{0.1} \leq 0.1$) in ML (left panel a-c) and OPA (right panel d-f). The scatter plot shows the relationship between the link capacities and the initial link flows in a homogeneous allocation strategy, where the capacity of a link is assumed to be proportional to its initial flow (circles) and after in the optimization-based approach of Section III (squares).

5.2.3 Brief summary

The results from the topology optimization based on the ML model and the comparative link capacity optimization provide an important contribution regarding the usefulness of a topological model (ML) in the optimization of a cascade resilient electrical network. Although ML is a relatively simple and abstract model (that does not account for the power flow laws and constraints of the electrical system), it is able to provide results that are consistent with a detailed and more realistic power flow model (OPA), when applied to the problem of network optimization against cascading failure. Most importantly, with respect to OPA it has the advantages

of simplicity and scalability. This provides impetus for the use of network-centric models to the study of ensemble characteristics of cascading failure in large power network systems.

5.3 Restoration optimization for enhanced system resilience – case study

The illustration of the Resilience Optimization Problem (ROP) and the heuristic scheduling algorithm proposed to solve it (Chapter 4) takes again the FPTN400 system (Figure 5:5) as a case study: however, in this case realistic power capacities of generators and transmission lines are used and the demands of all load buses are approximated by real data (see appended Paper [5]).

In the case study, we randomly select parts of the arcs of the network to be damaged. In addition, the repair costs of all the transmission lines are assumed to be constant and identical, and the cost limits $C(t)$ are assumed to be equal to the repair cost of a single arc: this means that only a single arc can be repaired at any given timeslot. It is noted that these assumptions can be relaxed to adapt to more realistic application cases.

We firstly consider repair optimization for a specific disruption scenario on the FPTN400, where 10% of network arcs (i.e. 22) are initially damaged. All the demand nodes are assumed to have identical weights in the optimization process. For the solution of the repair optimization problem, both the proposed heuristic dispatching rule (Chapter 4.3) and a classical MIP solver (i.e., Cplex MIP solver) are applied. Figure 5:13 reports the optimal restoration curves (i.e., network performance $F(t)$ as a function of time t) obtained by the dispatching rule (squares) and MIP (circles), respectively. It is found that the dispatching rule is able to obtain near optimal solutions: the recovery duration T is 5 (in arbitrary units) for both methods, and the system resilience $R(T)$ (Equation 4.3) is $R_{disp} = 0.731$ for the dispatching rule, and $R_{opt} = 0.753$ for MIP: the optimality gap between the two approaches is only 2.92%. Figure 5:14 provides a visualization of the optimal recovery plans obtained by the two methods. It is shown that the dispatching rule achieves very similar restoration plans to that of MIP. Both cases give high repair priority to those transmission lines which are unique connections to the demand nodes. More importantly, the dispatching rule is computationally much cheaper (6.9s) than MIP (20.5s).

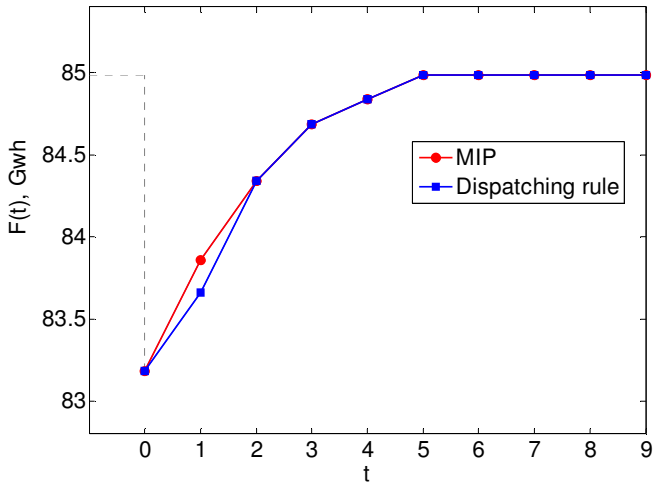


Figure 5:13 Optimal restoration curves obtained by the dispatching rule and MIP solver for the specific disruption scenario (10% links damaged) on the FPTN400.

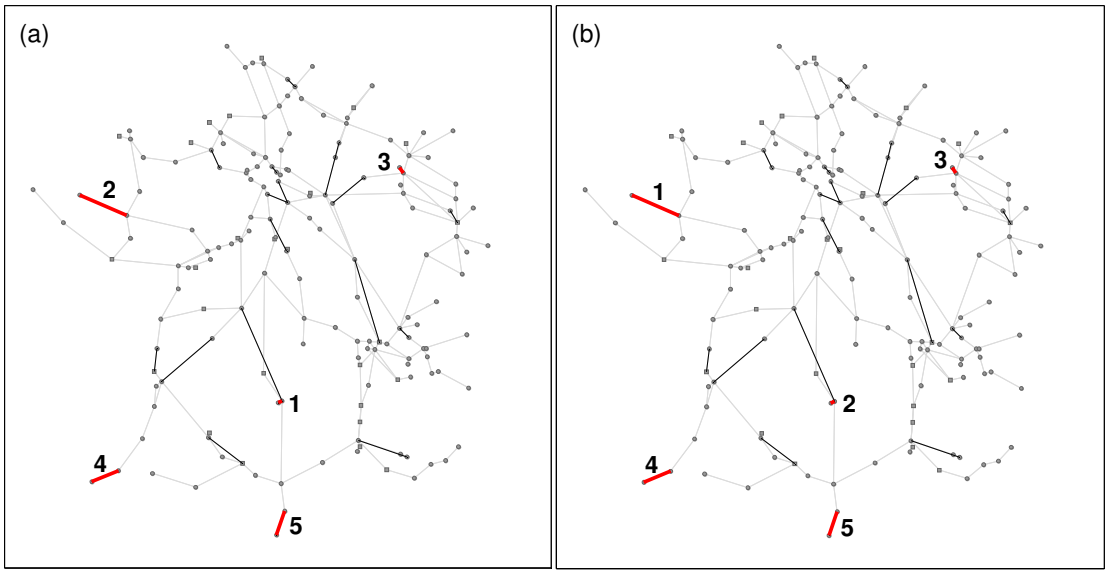


Figure 5:14 Visualization of the optimal recovery plans obtained by the dispatching rule (a) and MIP solver (b) for the specific disruption scenario (10% links damaged) on the FPTN400. The numbers indicate the optimal recovery timeslots of the five arcs marked by bold solid lines; black lines correspond to other failed arcs.

In order to further demonstrate the performance of the heuristic dispatching rule, we considered different levels of damage on the network (5% to 20% of arcs are randomly selected to be failed) and two different types of weights (i.e. of importance) for the demand nodes (i.e. w_j for $j \in V_D$): in the first class of demand nodes weights (namely, "Constant") each unit of flow received by demand nodes is weighed evenly across all the demand nodes; in the second class ('Priority'), some randomly chosen demand nodes are assigned higher value of w_j to represent higher priority. Table 5:4 provides the solutions and corresponding computational performances of the heuristic dispatching rule and the Cplex MIP solver for the ROP on the FPTN400. It is shown that the recovery time T provided by the heuristic dispatching rule is the same (for 5% and 10% cases) or slightly larger (for 15% and 20% cases) than the optimal solutions, and the relative optimality gaps between the two methods are less than 10% in most cases. Furthermore, the dispatching rule needs only, on average, the 10% of the computation time needed by the MIP solver for all the cases. These results indicate that the proposed heuristic dispatching rule is able to obtain high-quality sub-optimal (and optimal in some cases) solutions to the ROP, with much less computational cost compared with the Cplex MIP solver.

Table 5:4 Performances of the heuristic dispatching rule and the Cplex MIP solver on the FPTN400.

% of failed arcs (number)	w_j	Heuristic dispatching rule				Cplex MIP solver		
		Recovery time T	Opt. resilience	Solver time (s)	Opt. gap (%)	Recovery time T	Opt. resilience	Solver time (s)
5% (11)	Constant	2	0.917	4.69	4.28	2	0.958	20.30
5% (11)	Priority	2	0.921	4.75	6.40	2	0.984	20.94
10% (22)	Constant	5	0.731	6.90	2.92	5	0.753	40.50
10% (22)	Priority	5	0.852	8.60	0.00	5	0.852	46.32
15% (33)	Constant	14	0.646	20.45	5.42	12	0.683	110.16
15% (33)	Priority	14	0.685	26.40	13.07	12	0.788	224.45
20% (44)	Constant	15	0.569	70.31	9.97	13	0.632	632.42
20% (44)	Priority	15	0.626	75.46	8.08	13	0.681	1102.80

In particular, it is noted that the MIP solver may need much more time (e.g., days) to achieve optimal solutions for larger infrastructure systems (e.g., composed of thousands of nodes and links) or heavier disruption events (e.g., over 20% components damaged). Thus, it is unreasonable to expect the managers of the infrastructure systems to have access to unlimited computing resources or be willing to wait for several hours (or even several days) to determine their restoration plan. Consequently, the proposed heuristic dispatching rule represents an appealing tool for real-time restoration activities on larger scale CI systems.

5.4 Illustration of resilience-based component importance measures

The IEEE 30 Bus test system (Power system test case archive, 2014) is taken as reference case study for the proposed resilience-based CIMs of Chapter 4.4. This system (Figure 5:15) represents a portion of the American Electric Power System and is composed of 30 buses connected by 41 transmission lines. To carry out the analysis, each system component is transposed into a node or edge of the representative topological network. Three different physical types of nodes are considered: generator nodes (where the electricity flow is fed into the network), demand nodes (where customers are connected) and transfer or transmission nodes (without customers or sources).

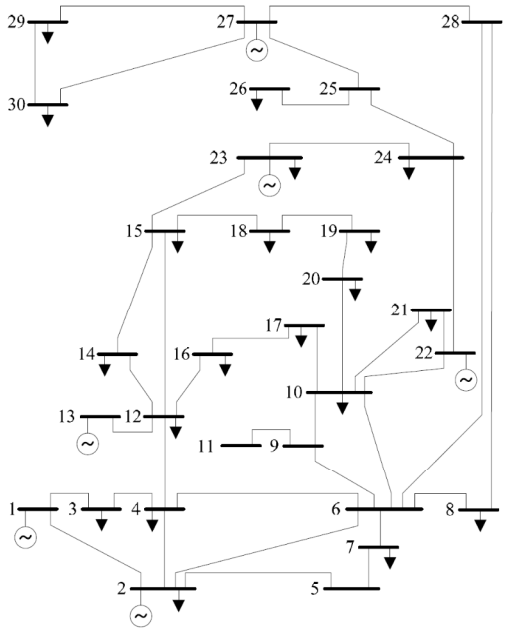


Figure 5:15 Single line diagram of the IEEE 30 Bus test system.

The simulation procedure introduced in Chapter 4.4.3 is, then, used to rank each component of the IEEE 30 Bus network according to the resilience-based criticality metrics introduced. Figure 5:16 illustrates the Cumulative Distribution Functions (CDFs) of T_{ij}^{opt} for five representative links (<1, 3>, <5, 7>, <27, 30>, <8, 28> and <10, 21>), obtained at step 5 of the procedure by applying the simulation algorithm proposed in Chapter 4.4.3 (for $\aleph = 1000$ samples). This Figure illustrates the probability that T_{ij}^{opt} is less than or equal to a given value x of interest. It can be seen that the optimal repair time associated with link <1, 3>, i.e. T_{13}^{opt}, will never be larger than 5 (square-line curve in Figure 5:16). Moreover, the curve for link <1, 3> always "dominates" the other curves. Therefore, this link should have the highest priority to be repaired in order to maximize system resilience.

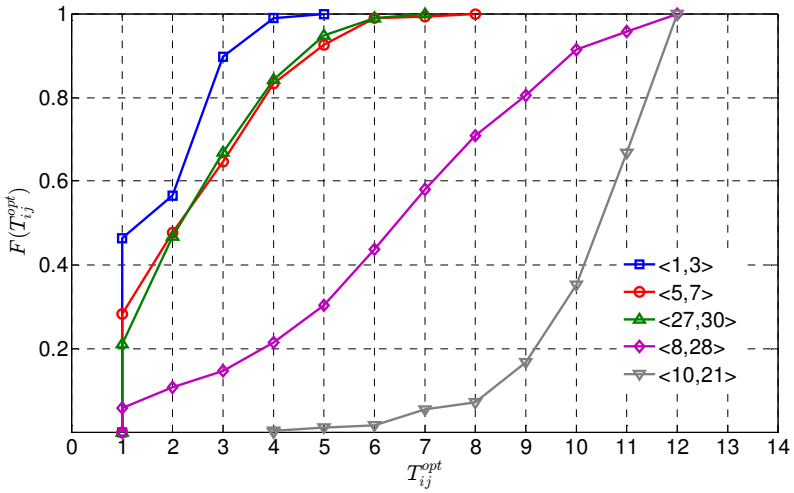


Figure 5:16 Cumulative probability distributions of the optimal repair time T_{ij}^{opt} for five representative links.

However, considering, e.g., links <5, 7> (circle line) and <27, 30> (triangle line) in Figure 5:16, it is not evident which one "dominates" the other, due to the intersection of their CDF curves. Thus, the CM-based ranking approach introduced in Chapter 4.4.4 is applied to rank the importance of the links. Figure 5:17 reports the Copeland scores of all the 41 links in the IEEE 30 Bus network, ordered in descending order, with link <1, 3> having the highest score, followed by links <2, 6>, <2, 4>, <10, 22> and so forth. Furthermore, it is found that two types of network links are more important in terms of T_{ij}^{opt}: i) the links which connect the generator nodes with the other two types of nodes (transmission nodes and demand nodes), e.g. links <2, 6>, <1, 3>, <12, 13> etc., and ii) the links which are the only ones connected to demand nodes, e.g. link <25, 26>. The restoration of these types of links is most likely able to augment the total amount of flow received by the demand nodes of the network: thus, high priority should be given to these links when considering the repair order of the failed links.

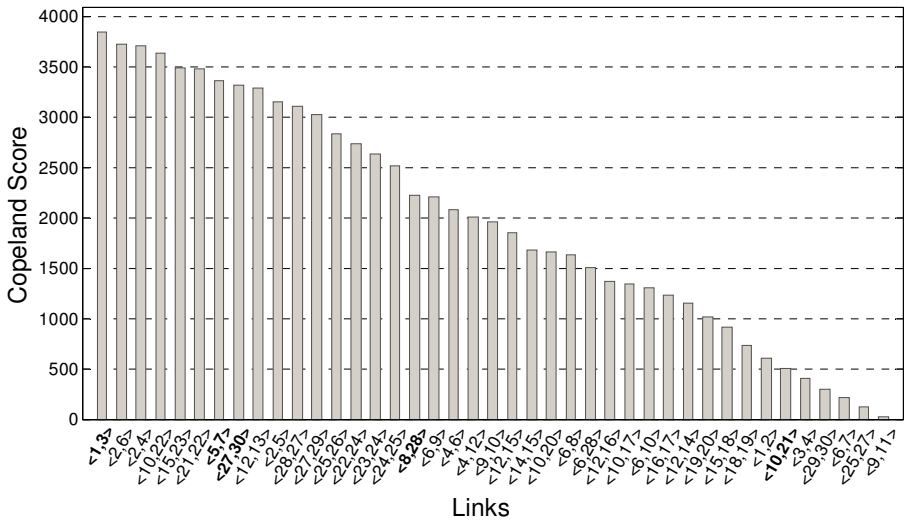


Figure 5:17 Copeland score ranking of the optimal repair time T_{ij}^{opt} for all IEEE 30 Bus network links.

Finally, Figure 5:18 reports the results based on the resilience reduction worth $RRW_{ij}(\Delta t_0)$ for all the links and for a delay time $\Delta t_0 = 3$ units. It is shown that <24, 25> is the most critical link in terms of RRW_{ij}, i.e. a delay in its restoration would cause the largest reduction in system resilience among all the network links; thus,

adequate resources should be given to make sure of its timely restoration. Besides, it is noted that the links with high Copeland scores in terms of the optimal repair time T_{ij}^{opt} also have high Copeland score ranking in terms of the resilience reduction worth RRW_{ij}: the correlation coefficient between the two Copeland scores is $r\left(C_{T_{ij}^{opt}}, C_{RRW_{ij}}\right) = 0.82$ for $\Delta t_0 = 3$.

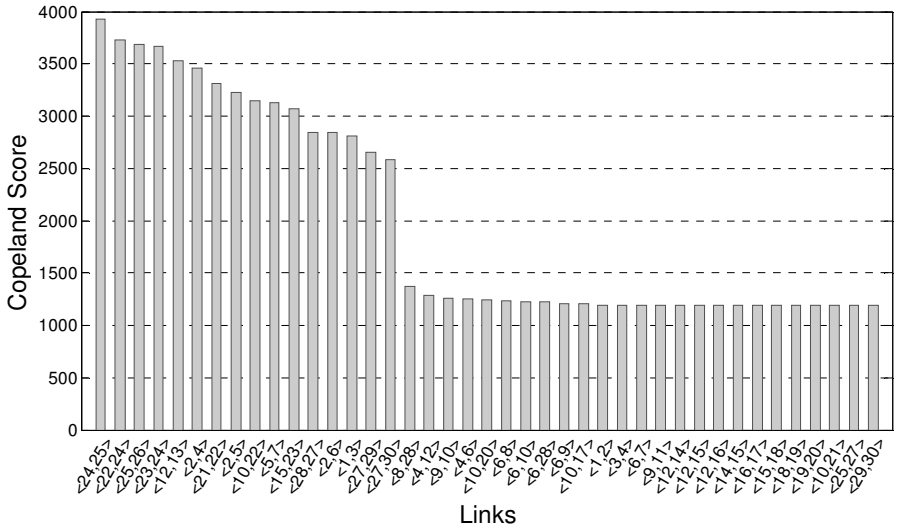


Figure 5:18 Copeland score ranking of the resilience reduction worth $RRW_{ij}(\Delta t_0 = 3)$ for all IEEE 30 Bus network links.

Chapter 6 Conclusions and future research

6.1 Conclusions

This dissertation focuses on the modelling, simulation, analysis and optimization of engineered critical infrastructure (CI) networks, with respect to their vulnerability and resilience to cascading failures. The entire state transition process of the CI system under disruptive events (i.e., stable, dynamic failure and system recovery state) has been considered. A comprehensive methodology has been developed, which combines: (i) the analysis of the structure and topology of the CI network represented by the interconnections among its components; (ii) the simulation of the CI network behavior in the presence of random failures and intentional attacks; (iii) the assessment of the CI vulnerability and resilience, with respect to cascading failures; (iv) the optimization of some characteristics of the CI network (e.g., its topology, link capacities, etc.) in order to maximize its robustness to cascading failures and its capability of recovering from disruptive events. The ultimate goal is to provide valuable insights for the safe planning and operation of large-scale complex CI systems against systemic failures.

A critical challenge related to the study of any real-life CI system lies in its inherent complexity; thus, well-defined system boundaries and simplifications of the system representation and analysis are usually required. Based on recent developments in the field of complex network theory and statistical clustering techniques, this dissertation has introduced a method for hierarchical representation and analysis of large-scale CI systems, which leads to the definition of different varied-size grained artificial networks. The availability of different scales of modeling resolution can be leveraged efficiently to facilitate the management of complexity in the analysis of large-scale CI systems. The computations of network node-pair reliability and the extended CIMs involving the IPTN380 have demonstrated the effectiveness of the proposed method.

The problem of CI protection against cascading failures has been addressed from a holistic system design perspective. Specifically, we have identified optimal relevant network properties, i.e., interconnectivity and link capacity allocation, by which the robustness of a CI network against cascading failures is maximized. For the simulation and analysis of the failure propagation in the optimization process, two different cascading failure modelling approaches of increasing complexity have been applied, for the sake of comparison: an abstract complex network-based model and a physical flow-based model (for electrical power grids), have been applied in the comparative study. This choice is partly motivated by the criticism often presented against the abstract modelling of cascading failures relying only on the resemblance of network topology, according to which the topological structure cannot be the only factor driving the functional state and the propagation of failures in a physical network. In our work, we have instead found that a relatively simple and abstract model (in particular, the Motter-Lai (ML) model) is indeed able to provide results that are consistent with a detailed and more realistic power flow model (in particular, the ORNL-PSerc-Alaska (OPA) model), when applied to the problem of network optimization against cascading failures. This has been demonstrated by extensive application of the compared approaches to the FPTN400 network. Such results provide impetus for the use of network theory-based models to the study of *ensemble* characteristics of cascading failures in large power network systems, due to

their advantages of simplicity and scalability. In all the cases, the optimization has been carried out by artificial intelligence based algorithms, in particular, the NSGA-II and NSBDE.

Resilience is another critical concept in the study of CI systems. Various definitions of "resilience" have been proposed for engineering and/or economic system analysis from different disciplines in the past decades. However, there is currently a lack of standardization and rigor when quantitatively defining this concept. In this study, we have rigorously introduced a new quantitative metric for system resilience, which embraces both the temporal and functional dimensions of system recovery. Based on this metric, a bi-level resilience optimization problem has been formulated for selecting proper recovery actions in order to enhance the resilience of infrastructure networks. This problem has been proven to be strongly NP-complete and, thus, it is computationally intensive, especially for large-scale infrastructure networks composed of thousands of nodes and links. We have solved this problem by proposing a heuristic dispatching rule, which has integrated fundamental concepts from network flows and project scheduling. The results of the case study involving the FPTN400 system have demonstrated that the proposed algorithm is able to produce high-quality sub-optimal solutions to the resilience optimization problem, with much less computational cost than the classical Cplex (MIP) solver based on a branch and cut algorithm.

Finally, two novel resilience-based component importance measures (CIMs) have been introduced in order to assess the criticality of network components from the perspective of their contribution to system resilience. The first resilience-based component importance measure, i.e. the optimal repair time (ORT), offers an explicit quantification of the priority that should be given to a failed component to be repaired and re-installed into the network. The second resilience-based component importance measure, i.e. the resilience reduction worth (RRW), quantifies the potential loss in optimal system resilience due to a delay in the repair time of a component. This measure can provide valuable information to guide the recovery process of a particular component: components with high values of RRW should be given high priority to their timely restoration, e.g. be assigned adequate restoration resources. The proposed CIMs have been tested and compared to classical centrality measures (e.g., shortest path betweenness, flow betweenness and random walk betweenness) on the IEEE 30 Bus test network: the results have shown that the classical betweenness centrality indices do not capture resilience criticality as do the resilience-based measures ORT and RRW.

6.2 Future research

Some limitations and open problems arising from this dissertation necessitate discussion for possible further study. Firstly, the hierarchical network representation model proposed in Chapter 2 is based on a recursive clustering where only the topological information is embraced in the affinity matrix. Other properties such as the geographical and functional relations of components could also be used to quantify the affinity between different components of a network system, depending on the context in which the model will be used. Besides, spectral clustering is adopted in Chapter 2 as one possible way to extract some inherent cluster-level structural properties and derive the hierarchical model, which sets the basis for a multi-scale criticality analysis. Yet, as many real adjacency matrices are sparse in nature, efficient existing methods to compute the eigenvectors of sparse matrices could be adopted (Golub and Van Loan, 2012).

In addition, some adjustments of the OPA model have been made in the comparison between the abstract ML model and the physical flow-based OPA model in Chapter 3. These adjustments ensure that we can use the

network tolerance parameter α as a common measure of transmission capacity for both models. However, the actual data concerning power generation and demands could be used (if available) both in the OPA validation and the optimization. Besides, performing optimizations using directly detailed and computationally intensive power flow models (e.g., embrace the so-called Manchester model (Nedic et al., 2006) and/or realistic trigger events such as natural hazard and malevolent targeted disruption (Dueñas-Osorio and Vemuru, 2009), into the cascade modelling framework) would enable a more thorough and comprehensive comparison of the two classes of approaches considered in this study.

Further, the resilience optimization model introduced in Chapter 4 focuses only on the optimal completion time of each failed component, in order to obtain insights about the importance that recovering each single component has in improving the resilience of the whole system; on the other hand, the duration of the repair of the failed components is not considered (i.e., the repair action is assumed to be instantaneous). This assumption could be relaxed to adapt to more realistic application cases by incorporating a repair model for a single failed component, in which the repair time of a component is stochastic (Xu et al., 2007) and/or related with the repair resources allocated to the component.

Finally, the focus of this dissertation is concentrated on single CI network systems; however, the interdependencies among civil infrastructure systems are ubiquitous and growing in number and strength. A paradigmatic example is represented by the power and communication networks (Little, 2002; Rosato et al., 2008): communication network nodes rely for power supply on the power stations and, reciprocally, the power stations function properly exchanging information through the communication network. This interdependency may lead to cascading failures between the networks and a relatively small failure could lead to a catastrophic breakdown of the system (Buldyrev et al., 2010). Over the past decade, there have been substantial conceptual and theoretical advances in the field of interdependent networks (Buldyrev et al., 2010; Zio and Sansavini, 2011b; Reis et al., 2014); however, most frameworks use highly simplified models of real networks, or theoretical network models to formulate the interdependencies problem. Attempting to understand and quantify the effects of interdependencies among various types of real-life engineered infrastructure systems in their response to systemic risks still constitute the fundamental challenge for CI protection.

References

Ahuja, R. K., Magnanti, T. L., & Orlin, J. B. (1993). *Network flows: theory, algorithms, and applications*.

Albert, R., & Barabási, A. L. (2002). Statistical mechanics of complex networks. *Reviews of modern physics*, *74*(1), 47.

Albert, R., Albert, I., & Nakarado, G. L. (2004). Structural vulnerability of the North American power grid. *Physical review E*, *69*(2), 025103.

Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. *Nature*, *406*(6794), 378-382.

Al-Sharrah, G. (2010). Ranking using the Copeland score: a comparison with the Hasse diagram. *Journal of chemical information and modeling*, 50(5), 785-791.

Amin, M. (2001). Toward self-healing energy infrastructure systems. *Computer Applications in Power, IEEE*, *14*(1), 20-28.

Amin, M. (2004). Balancing market priorities with security issues. *Power and Energy Magazine, IEEE*, *2*(4), 30-38.

Andrews, J. D., & Beeson, S. (2003). Birnbaum's measure of component importance for noncoherent systems. *Reliability, IEEE Transactions on*, 52(2), 213-219.

Apostolakis, G. E., & Lemon, D. M. (2005). A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Analysis*, *25*(2), 361-376.

Ash, J., & Newth, D. (2007). Optimizing complex networks for resilience against cascading failure. *Physica A: Statistical Mechanics and its Applications*, *380*, 673-683.

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering & System Safety*, *92*(6), 745-754.

Aven, T. (2011). On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. *Risk Analysis*, 31(4), 515-522.

Bae, K., & Thorp, J. S. (1999). A stochastic study of hidden failures in power system protection. *Decision Support Systems*, *24*(3), 259-268.

Baldick, R., Chowdhury, B., Dobson, I., Dong, Z., Gou, B., Hawkins, D., ... & Zhang, X. (2008, July). Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures. In *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE* (pp. 1-8). IEEE.

Barabási, A. L., & Albert, R. (1999). Emergence of scaling in random networks. *Science*, *286*(5439), 509-512.

Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2013). Resilience-based network component importance measures. *Reliability Engineering & System Safety*, 117, 89-97.

Battiston, S., Delli Gatti, D., Gallegati, M., Greenwald, B., & Stiglitz, J. E. (2007). Credit chains and bankruptcy propagation in production networks. *Journal of Economic Dynamics and Control*, *31*(6), 2061-2084.

Bienstock, D., & Mattia, S. (2007). Using mixed-integer programming to solve power grid blackout problems. *Discrete Optimization*, *4*(1), 115-141.

Birnbaum, Z. W. (1968). On the importance of different components in a multicomponent system (No. TR-54). WASHINGTON UNIV SEATTLE LAB OF STATISTICAL RESEARCH.

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., & Hwang, D. U. (2006). Complex networks: Structure and dynamics. *Physics reports*, *424*(4), 175-308.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management*, *15*(1), 50-59.

Bompard, E., Gao, C., Napoli, R., Russo, A., Masera, M., & Stefanini, A. (2009). Risk assessment of malicious attacks against power systems. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, *39*(5), 1074-1085.

Borgatti, S. P. (2005). Centrality and network flow. *Social networks*, 27(1), 55-71.

Bouleimen, K., & Lecocq, H. (2003). A new efficient simulated annealing algorithm for the resource-constrained project scheduling problem and its multiple mode version. *European Journal of Operational Research*, 149(2), 268-281.

Brucker, P., Drexl, A., Möhring, R., Neumann, K., & Pesch, E. (1999). Resource-constrained project scheduling: Notation, classification, models, and methods. *European journal of operational research*, 112(1), 3-41.

Bruneau, M., S. Chang, R. Eguchi, G. Lee, T. O' Rourke, A. Reinhorn, M. Shinozuka, K. Tierney, W. Wallace, and D. von Winterfeldt (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*, 19, pp. 737-38.

Buckle, P., Mars, G., & Smale, S. (2000). New approaches to assessing vulnerability and resilience. *Australian Journal of Emergency Management, 15*(2), 8-14.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, *464*(7291), 1025-1028.

Bush, G.W. (2003). Homeland Security Presidential Directive-7 (HSPD-7). Washington, D.C.

Carreras, B. A., Lynch, V. E., Dobson, I., & Newman, D. E. (2002). Critical points and transitions in an electric power transmission model for cascading failure blackouts. *Chaos: An interdisciplinary journal of nonlinear science*, *12*(4), 985-994.

Chang, S. E., McDaniels, T. L., Mikawoz, J., & Peterson, K. (2007). Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 Ice Storm. *Natural Hazards*, *41*(2), 337-358.

Chen, J., Thorp, J. S., & Dobson, I. (2005). Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model. *International Journal of Electrical Power & Energy Systems*, *27*(4), 318-326.

Cimellaro, G. P., Reinhorn, A. M., & Bruneau, M. (2010). Framework for analytical quantification of disaster resilience. *Engineering Structures*, 32(11), 3639-3649.

Coffrin, C., Van Hentenryck, P., & Bent, R. (2011, July). Strategic stockpiling of power system supplies for disaster recovery. In *Power and Energy Society General Meeting, 2011 IEEE* (pp. 1-8). IEEE.

COM (Commission of the European Communities) (2006). *COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. COM (2006) 787 final, Brussels.

Cotilla-Sanchez, E., Hines, P. D., Barrows, C., & Blumsack, S. (2012). Comparing the topological and electrical structure of the North American electric power infrastructure. *Systems Journal, IEEE*, *6*(4), 616-626.

Crucitti, P., Latora, V., & Marchiori, M. (2004). Model for cascading failures in complex networks. *Physical Review E*, *69*(4), 045104.

Crucitti, P., Latora, V., & Marchiori, M. (2005). Locating critical lines in high-voltage electrical power grids. *Fluctuation and Noise Letters*, *5*(02), L201-L208.

Crucitti, P., Latora, V., & Porta, S. (2006). Centrality measures in spatial networks of urban streets. *Physical Review E*, *73*(3), 036125.

Cupac, V., Lizier, J. T., & Prokopenko, M. (2013). Comparing dynamics of cascading failures between network-centric and power flow models. *International Journal of Electrical Power & Energy Systems*, *49*, 369-379.

Deb, K. (2001). *Multi-objective optimization using evolutionary algorithms* (Vol. 16). John Wiley & Sons.

Deb, K., Pratap, A., Agarwal, S., & Meyarivan, T. A. M. T. (2002). A fast and elitist multiobjective genetic algorithm: NSGA-II. *Evolutionary Computation, IEEE Transactions on*, *6*(2), 182-197.

Dilley, M., & Boudreau, T. E. (2001). Coming to terms with vulnerability: a critique of the food security definition. *Food policy*, *26*(3), 229-247.

Dobson, I. (2012). Estimating the propagation and extent of cascading line outages from utility data with a branching process. *Power Systems, IEEE Transactions on*, *27*(4), 2146-2155.

Dobson, I., Carreras, B. A., & Newman, D. E. (2005a). A loading-dependent model of probabilistic cascading failure. *Probability in the Engineering and Informational Sciences*, *19*(01), 15-32.

Dobson, I., Carreras, B. A., & Newman, D. E. (2005b, January). Branching Process Models for the Exponentially Increasing Portions of Cascading Failure Blackouts. In *HICSS*.

Dobson, I., Carreras, B. A., Lynch, V. E., & Newman, D. E. (2007). Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *17*(2), 026103.

Dobson, I., Carreras, B. A., Lynch, V. E., Nkei, B., & Newman, D. E. (2005c). Estimating failure propagation in models of cascading blackouts. *Probability in the Engineering and Informational Sciences*, *19*(04), 475-488.

Dobson, I., Carreras, B., Lynch, V., & Newman, D. (2001, January). An initial model for complex dynamics in electric power system blackouts. In *2013 46th Hawaii International Conference on System Sciences* (Vol. 2, pp. 2017-2017). IEEE Computer Society.

Dueñas-Osorio, L., & Vemuru, S. M. (2009). Cascading failures in complex infrastructure systems. *Structural safety*, *31*(2), 157-167.

EDF. (2013). En direct de nos centrales, http://france.edf.com/france-45634.html, Retrieved Avril, 2013.

Ellis, J., Fisher, D., Longstaff, T., Pesante, L., & Pethia, R. (1997). *Report to the President's Commission on Critical Infrastructure Protection* (No. CMU/SEI-97-SR-00333). Carnegie-Mellon Univ., Pittsburgh, PA. Software Engineering Inst.

Erdös, Paul and Alfred Rényi (1959). On random graphs I. Math. *Debrecen*, *6*, 290-297.

Espiritu, J. F., Coit, D. W., & Prakash, U. (2007). Component criticality importance measures for the power industry. *Electric Power Systems Research*, 77(5), 407-420.

Eum, S., Arakawa, S. I., & Murata, M. (2008, September). Traffic dynamic in modularity structure of complex networks. In *Broadband Communications, Networks and Systems, 2008. BROADNETS 2008. 5th International Conference on* (pp. 390-395). IEEE.

Eusgeld, I., Kröger, W., Sansavini, G., Schläpfer, M., & Zio, E. (2009). The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliability Engineering & System Safety*, *94*(5), 954-963.

Filippone, M., Camastra, F., Masulli, F., & Rovetta, S. (2008). A survey of kernel and spectral methods for clustering. *Pattern recognition*, *41*(1), 176-190.

Fitzmaurice, R., Cotilla-Sanchez, E., & Hines, P. (2012, July). Evaluating the impact of modeling assumptions for cascading failure simulation. In *Power and Energy Society General Meeting, 2012 IEEE* (pp. 1-8). IEEE.

Freeman, L. C. (1979). Centrality in social networks conceptual clarification. *Social networks*, *1*(3), 215-239.

Freeman, L. C., Borgatti, S. P., & White, D. R. (1991). Centrality in valued graphs: A measure of betweenness based on network flow. *Social networks*, 13(2), 141-154.

Fussell, J. B. (1975). How to hand-calculate system reliability and safety characteristics. *Reliability, IEEE Transactions on*, *24*(3), 169-174.

Gandini, A. (1990). Importance and sensitivity analysis in assessing system reliability. *Reliability, IEEE Transactions on*, 39(1), 61-70.

Gertsbakh, I., & Shpungin, Y. (2008). Network reliability importance measures: combinatorics and monte carlo based computations. *WSEAS Trans Comp*, 4(7), 216-227.

Golub, G. H., & Van Loan, C. F. (2012). *Matrix computations* (Vol. 3). JHU Press.

Gómez C., Sánchez-Silva M., and Duenas-Osorio L. (2011). Clustering methods for risk assessment of infrastructure network systems. *Applications of Statistics and Probability in Civil Engineering*. Faber, Köhler and Nishijima (eds). ISBN 978-0-415-66986-3.

Grimmett, G. (1999). Percolation Springer-Verlag. *Berlin (Second edition)*.

Grubesic, T. H., Matisziw, T. C., Murray, A. T., & Snediker, D. (2008). Comparative approaches for assessing network vulnerability. *International Regional Science Review*, *31*(1), 88-112.

Guimera, R., Arenas, A., Díaz-Guilera, A., & Giralt, F. (2002). Dynamical properties of model communication networks. *Physical Review E*, *66*(2), 026704.

Gutfraind, A. (2010). Optimizing topological cascade resilience based on the structure of terrorist networks. *PloS one*, *5*(11), e13448.

Haimes, Y. Y. (2006). On the definition of vulnerabilities in measuring risks to infrastructures. *Risk Analysis*, *26*(2), 293-296.

Haimes, Y. Y., Crowther, K., & Horowitz, B. M. (2008). Homeland security preparedness: balancing protection with resilience in emergent systems. *Systems Engineering*, 11(4), 287-308.

Hansson, S. O., & Helgesson, G. (2003). What is stability?. *Synthese*, *136*(2), 219-235.

Hartmann, S. (1998). A competitive genetic algorithm for resource-constrained project scheduling. *Naval Research Logistics (NRL)*, 45(7), 733-750.

Helbing, D. (2013). Globally networked risks and how to respond. *Nature*, 497(7447), 51-59.

Henry, D., & Emmanuel Ramirez-Marquez, J. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering & System Safety*, 99, 114-122.

Hines, P., & Blumsack, S. (2008, January). A centrality measure for electrical networks. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual* (pp. 185-185). IEEE.

Hines, P., Apt, J., & Talukdar, S. (2009). Large blackouts in North America: Historical trends and policy implications. *Energy Policy*, *37*(12), 5249-5259.

Hines, P., Cotilla-Sanchez, E., & Blumsack, S. (2010). Do topological models provide good information about electricity infrastructure vulnerability?. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *20*(3), 033122.

Holling, C. (1973). Resilience and Stability of Ecological Systems, *Annual Review of Ecology and Systematics*, pp. 1-23.

Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Limited, Aldershot, UK.

Holme, P. (2002). Edge overload breakdown in evolving networks. *Physical Review E*, *66*(3), 036119.

Holme, P., & Kim, B. J. (2002). Vertex overload breakdown in evolving networks. *Physical Review E*, *65*(6), 066109.

Holme, P., Kim, B. J., Yoon, C. N., & Han, S. K. (2002). Attack vulnerability of complex networks. *Physical Review E*, *65*(5), 056109.

Holmgren, Å. J. (2006). Using graph models to analyze the vulnerability of electric power networks. *Risk analysis*, *26*(4), 955-969.

Iyer, S. M., Nakayama, M. K., & Gerbessiotis, A. V. (2009). A Markovian dependability model with cascading failures. *Computers, IEEE Transactions on*, *58*(9), 1238-1249.

Jain, A. K., Murty, M. N., & Flynn, P. J. (1999). Data clustering: a review. *ACM computing surveys (CSUR)*, *31*(3), 264-323.

Jarboui, B., Damak, N., Siarry, P., & Rebai, A. (2008). A combinatorial particle swarm optimization for solving multi-mode resource-constrained project scheduling problems. *Applied Mathematics and Computation*, 195(1), 299-308.

Jenelius, E. (2009). Network structure and travel patterns: explaining the geographical disparities of road network vulnerability. *Journal of Transport Geography*, *17*(3), 234-244.

Jenelius, E., Petersen, T., & Mattsson, L. G. (2006). Importance and exposure in road network vulnerability analysis. *Transportation Research Part A: Policy and Practice*, 40(7), 537-560.

Johansson, J., & Hassel, H. (2010). An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering & System Safety*, *95*(12), 1335-1344.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk analysis*, *1*(1), 11-27.

Karrer, B., Levina, E., & Newman, M. E. (2008). Robustness of community structure in networks. *Physical Review E*, *77*(4), 046119.

Kempe, D., Kleinberg, J., & Tardos, É. (2003, August). Maximizing the spread of influence through a social network. In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 137-146). ACM.

Kim, D. H., & Motter, A. E. (2008a). Fluctuation-driven capacity distribution in complex networks. *New Journal of Physics*, *10*(5), 053022.

Kim, D. H., & Motter, A. E. (2008b). Resource allocation pattern in infrastructure networks. *Journal of Physics A: Mathematical and Theoretical*, *41*(22), 224019.

Kinney, R., Crucitti, P., Albert, R., & Latora, V. (2005). Modeling cascading failures in the North American power grid. *The European Physical Journal B-Condensed Matter and Complex Systems*, *46*(1), 101-107.

Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety*, *93*(12), 1781-1787.

Kröger, W., & Zio, E. (2011). Introduction and definition of key term. *Vulnerable systems*. Springer.

Latora, V., & Marchiori, M. (2001). Efficient behavior of small-world networks.*Physical review letters*, *87*(19), 198701.

Latora, V., & Marchiori, M. (2005). Vulnerability and protection of infrastructure networks. *Physical Review E*, *71*(1), 015103.

Latora, V., & Marchiori, M. (2007). A measure of centrality based on network efficiency. *New Journal of Physics*, *9*(6), 188.

Levitin, G., Podofillini, L. and Zio, E. (2003). Generalized importance measures for multistate elements based on performance level restrictions. *Reliability Engineering and System Safety*, 82, 63-73.

Lewis, T. G. (2006). *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons.

Li, P., Wang, B. H., Sun, H., Gao, P., & Zhou, T. (2008). A limited resource model of fault-tolerant capability against cascading failure of complex network. *The European Physical Journal B-Condensed Matter and Complex Systems*,*62*(1), 101-104.

Li, Y. F., Sansavini, G., & Zio, E. (2013). Non-dominated sorting binary differential evolution for the multi-objective optimization of cascading failures protection in complex networks. *Reliability Engineering & System Safety*, *111*, 195-205.

Little, R. G. (2002). Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. *Journal of Urban Technology*, *9*(1), 109-123.

Masucci, A. P., Smith, D., Crooks, A., & Batty, M. (2009). Random planar graphs and the London street network. *The European Physical Journal B-Condensed Matter and Complex Systems*, *71*(2), 259-271.

McCarthy, J. A., Brashear, J. P., Pommerening, C., Siegel, J. L., Creel, J. T., Ryan, T. P., ... & Clark, L. C. (2005). *Critical Infrastructure Protection in the National Capital Region - Risk-Based Foundations for Resilience and Sustainability*. Final Report. Arlington, VA: George Mason University.

McDaniels, T., Chang, S., Peterson, K., Mikawoz, J., & Reed, D. (2007). Empirical framework for characterizing infrastructure failure interdependencies. *Journal of Infrastructure Systems*, *13*(3), 175-184.

Merkle, D., Middendorf, M., & Schmeck, H. (2002). Ant colony optimization for resource-constrained project scheduling. *Evolutionary Computation, IEEE Transactions on*, 6(4), 333-346.

Merlin, V. R., & Saari, D. G. (1997). Copeland method II: Manipulation, monotonicity, and paradoxes. *Journal of Economic Theory*, 72(1), 148-172.

Motter, A. E. (2004). Cascade control and defense in complex networks. *Physical Review Letters*, *93*(9), 098701.

Motter, A. E., & Lai, Y. C. (2002). Cascade-based attacks on complex networks. *Physical Review E*, *66*(6), 065102.

Najjar, W., & Gaudiot, J. L. (1990). Network resilience: a measure of network fault tolerance. *Computers, IEEE Transactions on*, 39(2), 174-181.

Natvig, B., Huseby, A. B., & Reistadbakk, M. O. (2011). Measures of component importance in repairable multistate systems—a numerical study. *Reliability Engineering & System Safety*, 96(12), 1680-1690.

Nedic, D. P., Dobson, I., Kirschen, D. S., Carreras, B. A., & Lynch, V. E. (2006). Criticality in a cascading failure blackout model. *International Journal of Electrical Power & Energy Systems*, *28*(9), 627-633.

Newman, M. E. (2003). The structure and function of complex networks. *SIAM review*, *45*(2), 167-256.

Newman, M. E. (2005). A measure of betweenness centrality based on random walks. *Social networks*, 27(1), 39-54.

Newman, M. E., Forrest, S., & Balthrop, J. (2002). Email networks and the spread of computer viruses. *Physical Review E*, *66*(3), 035101.

Nieminen, J. (1974). On the centrality in a graph. *Scandinavian Journal of Psychology*, 15(1), 332-336.

Obama, B. (2013). *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*. Washington, D.C.

Omer, M., Nilchiani, R., & Mostashari, A. (2009). Measuring the resilience of the trans-oceanic telecommunication cable system. *Systems Journal, IEEE*, 3(3), 295-303.

Ouyang, M., & Dueñas-Osorio, L. (2012). Time-dependent resilience assessment and improvement of urban infrastructure systems. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 22(3), 033122.

Pidd H. (2012). India blackouts leave 700 million without power. The Guardian, 31 July 2012.

Pinedo, M. L. (2012). *Scheduling: theory, algorithms, and systems*. Springer.

Pomerol, J. C., & Barba-Romero, S. (2000). *Multicriterion decision in management: principles and practice* (Vol. 25). Springer.

Porter, M. A., Onnela, J. P., & Mucha, P. J. (2009). Communities in networks.*Notices of the AMS*, *56*(9), 1082-1097.

Purchala, K., Meeus, L., Van Dommelen, D., & Belmans, R. (2005, June). Usefulness of DC power flow for active power flow analysis. In *Power Engineering Society General Meeting, 2005. IEEE* (pp. 454-459). IEEE.

Pursiainen, C. (2009). The challenges for European critical infrastructure protection. *European Integration*, 31(6), 721-739.

Ramirez-Marquez, J. E., & Coit, D. W. (2005). Composite importance measures for multi-state systems with multi-state components. *Reliability, IEEE Transactions on*, 54(3), 517-529.

Ramirez-Marquez, J. E., & Coit, D. W. (2007). Multi-state component criticality analysis for reliability improvement in multi-state systems. *Reliability Engineering & System Safety*, 92(12), 1608-1619.

Reed, D. A., Kapur, K. C., & Christie, R. D. (2009). Methodology for assessing the resilience of networked infrastructure. *Systems Journal, IEEE*, 3(2), 174-180.

Reis, S. D., Hu, Y., Babino, A., Andrade Jr, J. S., Canals, S., Sigman, M., & Makse, H. A. (2014). Avoiding catastrophic failure in correlated networks of networks. *Nature Physics*.

Ren, H., & Dobson, I. (2008). Using Transmission Line Outage Data to Estimate Cascading Failure Propagation in an Electric Power System. *IEEE Trans. on Circuits and Systems*, *55*(9), 927-931.

Rosato, V., Bologna, S., & Tiriticco, F. (2007). Topological properties of high-voltage electrical transmission networks. *Electric Power Systems Research*, *77*(2), 99-105.

Rosato, V., Issacharoff, L., Tiriticco, F., Meloni, S., Porcellinis, S., & Setola, R. (2008). Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures*, *4*(1), 63-79.

Rose, A. (2007). Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. *Environmental Hazards*, 7(4), 383-398.

Rosenkrantz, D. J., Goel, S., Ravi, S. S., & Gangolly, J. (2009). Resilience metrics for service-oriented networks: A service allocation approach. *Services Computing, IEEE Transactions on*, 2(3), 183-196.

RTE. (2011). Le Réseau de Transport d'Electricité 400 kV, 2011, http://www.rte-france.com

Sachtjen, M. L., Carreras, B. A., & Lynch, V. E. (2000). Disturbances in a power transmission system. *Physical Review E*, *61*(5), 4877.

Sales-Pardo, M., Guimera, R., Moreira, A. A., & Amaral, L. A. N. (2007). Extracting the hierarchical organization of complex systems. *Proceedings of the National Academy of Sciences*, *104*(39), 15224-15229.

Schölkopf, B., Smola, A., & Müller, K. R. (1998). Nonlinear component analysis as a kernel eigenvalue problem. *Neural computation*, *10*(5), 1299-1319.

Shao, F. M., Shen, X., & Ho, P. H. (2005). Reliability optimization of distributed access networks with constrained total cost. *Reliability, IEEE Transactions on*, *54*(3), 421-430.

Simonsen, I., Buzna, L., Peters, K., Bornholdt, S., & Helbing, D. (2008). Transient dynamics increasing network vulnerability to cascading failures. *Physical review letters*, *100*(21), 218701.

Smith, W. E. (1956). Various optimizers for single-stage production. *Naval Research Logistics Quarterly*, 3(1-2), 59-66.

Strogatz, S. H. (2001). Exploring complex networks. *Nature*, *410*(6825), 268-276.

Talukdar, S. N., Apt, J., Ilic, M., Lave, L. B., & Morgan, M. G. (2003). Cascading failures: survival versus prevention. *The Electricity Journal*, *16*(9), 25-31.

Thadakamaila, H. P., Raghavan, U. N., Kumara, S., & Albert, R. (2004). Survivability of multiagent-based supply networks: a topological perspect. *Intelligent Systems, IEEE*, *19*(5), 24-31.

U.C.T.E, (2004). Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy. *Tech. Rep.* Union for the Coordination of Transmission of Electricity.

U.C.T.E, (2007), Final Report System Disturbance on 4 Nov. 2006. *Tech. Rep.*, Union for the Coordination of Transmission of Electricity.

U.S.-CA (April 2004). Final Report on the August 14th blackout in the United States and Canada. *Tech. Rep.*, United States Department of Energy and National Resources Canada.

Van der Borst, M., & Schoonakker, H. (2001). An overview of PSA importance measures. *Reliability Engineering & System Safety*, 72(3), 241-245.

Van Dongen, S. M. (2000). *Graph clustering by flow simulation*.

Von Luxburg, U. (2007). A tutorial on spectral clustering. *Statistics and computing*, *17*(4), 395-416.

Vugrin, E. D., Warren, D. E., Ehlen, M. A., & Camphouse, R. C. (2010). A framework for assessing the resilience of infrastructure and economic systems. In *Sustainable and Resilient Critical Infrastructure Systems* (pp. 77-116). Springer Berlin Heidelberg.

Wang, B., & Kim, B. J. (2007). A high-robustness and low-cost model for cascading failures. *EPL (Europhysics Letters)*, *78*(4), 48001.

Wang, H., & Thorp, J. S. (2001). Optimal locations for protection system enhancement: a simulation of cascading outages. *Power Delivery, IEEE Transactions on*, *16*(4), 528-533.

Wang, L., Fu, X., Menhas, M. I., & Fei, M. (2010). A modified binary differential evolution algorithm. In *Life System Modeling and Intelligent Computing* (pp. 49-57). Springer Berlin Heidelberg.

Wang, W., Loman, J., & Vassiliou, P. (2004). Reliability importance of components in a complex system. In *Reliability and Maintainability*, 2004 Annual Symposium-RAMS (pp. 6-11). IEEE.

Wang, X. F., & Xu, J. (2004). Cascading failures in coupled map lattices. *Physical Review E*, *70*(5), 056113.

Wang, Z., Scaglione, A., & Thomas, R. J. (2012, January). A Markov-transition model for cascading failures in power grids. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2115-2124). IEEE.

Watts, D. J. (2002). A simple model of global cascades on random networks. *Proceedings of the National Academy of Sciences*, *99*(9), 5766-5771.

Watts, D. J. (2004). *Six degrees: The science of a connected age*. WW Norton & Company.

Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of 'small-world'networks. *Nature*, *393*(6684), 440-442.

Weichselgartner, J. (2001). Disaster mitigation: the concept of vulnerability revisited. *Disaster Prevention and Management*, *10*(2), 85-95.

Weron, R., & Simonsen, I. (2006). Blackouts, risk, and fat-tailed distributions. In *Practical Fruits of Econophysics* (pp. 215-219). Springer Tokyo.

Wu, J. J., Gao, Z. Y., & Sun, H. J. (2006). Cascade and breakdown in scale-free networks with community structure. *Physical Review E*, *74*(6), 066111.

Xiao, H., & Yeh, E. M. (2011, June). Cascading link failure in the power grid: A percolation-based analysis. In *Communications Workshops (ICC), 2011 IEEE International Conference on* (pp. 1-6). IEEE.

Xu, N., Guikema, S. D., Davidson, R. A., Nozick, L. K., Çağnan, Z., & Vaziri, K. (2007). Optimizing scheduling of post-earthquake electric power restoration tasks. *Earthquake engineering & structural dynamics*, *36*(2), 265-284.

Zhao, K., Kumar, A., Harrison, T. P., & Yen, J. (2011). Analyzing the resilience of complex supply network topologies against random and targeted disruptions.*Systems Journal, IEEE*, *5*(1), 28-39.

Zio, E. (2007). From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures. *International Journal of Critical Infrastructures*, *3*(3), 488-508.

Zio, E. (2009). Reliability engineering: Old problems and new challenges. *Reliability Engineering & System Safety*, *94*(2), 125-141.

Zio, E., & Piccinelli, R. (2010). Randomized flow model and centrality measure for electrical power transmission network analysis. *Reliability Engineering & System Safety*, 95(4), 379-385.

Zio, E., & Sansavini, G. (2011a). Component criticality in failure cascade processes of network systems. *Risk Analysis*, *31*(8), 1196-1210.

Zio, E., & Sansavini, G. (2011b). Modeling interdependent network systems for identifying cascade-safe operating margins. *Reliability, IEEE Transactions on*, *60*(1), 94-101.

Zio, E., Sansavini, G., Maja, R., & Marchionni, G. (2008). An analytical approach to the safety of road networks. *International Journal of Reliability, Quality and Safety Engineering*, *15*(01), 67-76.

Zitzler, E., Laumanns, M., & Bleuler, S. (2004). A tutorial on evolutionary multiobjective optimization. In *Metaheuristics for multiobjective optimization* (pp. 3-37). Springer Berlin Heidelberg.

Part II

Appended papers

Paper [1] Y.-P. Fang, E. Zio. "Unsupervised spectral clustering for hierarchical modelling and criticality analysis of complex networks." Reliability Engineering and System Safety, 116:64-74, 2013

Reliability Engineering and System Safety 116 (2013) 64–74

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Unsupervised spectral clustering for hierarchical modelling and criticality analysis of complex networks

Yi-Ping Fang [a,*], Enrico Zio [a,b]

[a] Chair on Systems Science and the Energetic Challenge, Ecole Centrale Paris and Supelec, Paris 92295, France
[b] Energy Department, Politecnico di Milano, Milano, Italy

ARTICLE INFO

Article history:
Received 23 August 2012
Received in revised form
24 January 2013
Accepted 21 February 2013
Available online 16 March 2013

Keywords:
Critical infrastructures
Complex networks
Criticality analysis
Centrality measures
Spectral clustering
Hierarchical modelling

ABSTRACT

Infrastructure networks are essential to the socioeconomic development of any country. This article applies clustering analysis to extract the inherent structural properties of realistic-size infrastructure networks. Network components with high criticality are identified and a general hierarchical modelling framework is developed for representing the networked system into a scalable hierarchical structure of corresponding fictitious networks. This representation makes a multi-scale criticality analysis possible, beyond the widely used component-level criticality analysis, whose results obtained from zoom-in analysis can support confident decision making.

1. Introduction

Engineered critical infrastructures are 'a network of independent, large-scale, man-made systems…that function collaboratively and synergistically to produce a continuous flow of essential goods (e.g. energy, data, water…) and services (e.g. banking, healthcare, transportation)' [1] vital to the economy, security and well-being of any country. These systems are exposed to multiple hazards and threats, some of which are even unexpected and emergent, so that a complete analysis by exhaustive treatment cannot be guaranteed. Furthermore, the infrastructure networks consist of a large number of elements whose interactions are not easily modeled and quantified. In practice, then, the performance and reliability assessment of such 'complex' systems has proved to be a non-trivial task.

The theory of complex networks has in recent years emerged as a valid tool for describing, modelling and quantifying complex systems in many branches of science [2–5]. Based on the network topology and its treatment by tools of graph theory, various statistical measures have been introduced to evaluate the global structural properties of the network and quantify the importance of the individual elements in the structure of the system [6–8]. While global performance indicators encompass the static characteristics of the whole network, the importance of the different elements in the network can be seen from the point of view of their individual connectivity efficiency and/or their contribution to the propagation of failures through the system network of connections [9–11]. Among these measures, classical and relevant statistics are the network efficiency [12–14], which evaluates the connectivity of the whole network, and the topological centrality measures including degree centrality (*CD*) [16,17], closeness centrality (*CC*) [15,17], betweenness centrality (*CB*) [17] and information centrality (*CI*) [18,19], which rely on topological information to qualify the importance of individual network elements.

On the other hand, recent studies suggest that many real complex networks exhibit a modularized organization [20]. In many cases, these modularized structures are found to correspond to functional units within networks (ecological niches in food webs, modules in biochemical networks) [21]. Broadly speaking, clusters (also called communities or modules) are found in the network, forming groups of elements that are densely interconnected with each other but only sparsely connected with the rest of the network. The study of the clustered structure of the network of a critical infrastructure is of particular interest because such structure can provide a protection for the system against attacks from an intruder [22], reduce the effects of cascade failures [23] and point at important heterogeneities within the network that may not be registered via network level measures [21]. Finally, hierarchically modularized organization, which is a central idea about the life process in biology, is found to be also an internal structure of many technological networks [24], and can be utilized

* Corresponding author. Tel.: +33 65224 0019.
E-mail address: yiping.fang@ecp.fr (Y.-P. Fang).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.02.021

Nomenclature

V	set of network nodes
E	set of network edges
$G(V, E)$	a network with set of nodes V and edges E
A	adjacency matrix of network
s_{ij}	similarity measure between node i and j
S	similarity matrix of network
L_{sys}	normalized graph Laplacian matrix
Q	network modularity index
SSE	sum of square error
D	network degree matrix
DB	Davies–Bouldin index of clustering
$Dunn$	Dunn index of clustering
C_k	cluster k of network $G(V, E)$
N_k	the central node of cluster k
n	number of network nodes
m	number of network edges
n_k	number of nodes in cluster k
$\Lambda^{(k)}$	set of fictitious nodes at level k
$E^{(k)}$	set of fictitious edges at level k
$G^{(k)}(\Lambda^{(k)},E^{(k)})$	fictitious network at level k of the hierarchy
$E(G)$	topology efficiency of network G
$V_i^{(k)}$	node i of the fictitious network at level k of the hierarchy
$C^I_{V_i^{(k)}}$	information centrality of node $V_i^{(k)}$
d_{ij}	shortest path between node i and j

to model these complex systems for their understanding and analysis [25].

The objective of the work presented in this paper is twofold. First, to propose clustering analysis for extracting some inherent structural properties of a network of a critical infrastructure and, second to adopt a scheme of successive clustering to obtain a hierarchical model made of different varied-size grained virtual networks which can be exploited to perform zoom-in assessments, focusing on the most relevant clusters in the virtual networks at each level of the hierarchy.

The remainder of this paper is organized as follows: Section 2 presents the proposed spectral clustering analysis, taking the structure of the Italian 380 kV power transmission network as an example for illustration; in Section 3, hierarchical modelling of a complex network is first introduced, and then multi-scaled criticality analyses are performed on the hierarchical model; conclusions are drawn in Section 4.

2. Clustering analysis

2.1. Network representation

Graph theory provides a natural framework for the mathematical representation of complex networks. A graph is an ordered pair $G(V,E)$comprising a set of vertices (nodes)$V=v_1,v_2,\ldots,v_n$ together with a set of edges (also called arcs or links) $E=e_1,e_2,\ldots,e_m$, which are two-element subsets of V. The network structure is usually defined by the $n\times n$ *adjacency matrix*, which defines which two nodes are connected by assigning a 1 to the corresponding element of the matrix; otherwise, the value in the matrix is 0 if there is no connection between the two nodes. As described, this type of graph is unweighted and undirected. A graph is weighted if a value (weight) is assigned to each edge representing properties of the connection like costs, lengths, capacities, etc. For example, the *matrix of physical distances* is often used in conjunction with the *adjacency matrix* to describe a network also with respect to its spatial dimension [12,26].

In this paper, we take an exemplification of the analyses proposed on the 380 kV Italian power transmission network (Fig. 1). This network is a branch of the high-voltage-level transmission, which can be modeled as a graph of $n=127$ nodes connected by $m=171$ links [7]·[27], defined by its $n\times n$ adjacency (connection) matrix A whose entries $[a_{ij}]$ are 1 if there is an edge joining node i to node j or 0 otherwise. It is important to underline that only the topology of the physical system is taken as reference and used in the analyses, so that the hierarchical model and clustering relate only on the network structure with no specific relation to the electrical properties of the system. The sub-network for Sardinia is not considered to ensure that the network is connected in the sense of a topological space.

2.2. Unsupervised spectral clustering algorithm

Cluster analysis aims at identifying patterns around which communities of elements in the network can be grouped, emerging implicit information in the network structure [28]. Framed as an unsupervised multiple classification problem [29], clustering has been an essential undertaking in the context of explorative data mining and also a common technique for statistical data analysis used in many fields such as machine learning, pattern recognition, image analysis, information retrieval, and bioinformatics [30]. Theoretically, based on a similarity (affinity) measure s_{ij}between pairs of data points (i,j), which is usually a measure of distance between i and j, most clustering approaches seek to achieve a minimum or maximum similarity value through an iterative process of vertex grouping [25,28]. Different similarity definitions can lead to different cluster partitioning of the network.

The detailed description of the different clustering methods is beyond the scope of this article. For a systematic and synthetic review, the reader is encouraged to look at [28,30,31]. For the purpose of the analyses presented in this paper, we adopt the unsupervised spectral clustering algorithm (USCA) [32], which is invariant to cluster shapes and densities and simple to implement. The USCA makes use of the spectrum (eigenvalues) of the similarity matrix of the data to perform dimensionality reduction before Fuzzy k-means (FKM)-clustering in fewer dimensions. Schematically, it is performed by the following steps [32]:

Unsupervised spectral clustering algorithm

Input: Similarity matrix $S\in\mathbb{R}^{n\times n}$

1. Compute the normalized graph Laplacian matrix L_{sym}
2. Compute the first k eigenvalues $\lambda_1,\lambda_2,\ldots,\lambda_k$ and corresponding eigenvectors $\overline{u}_1,\overline{u}_2,\ldots,\overline{u}_k$of matrix L_{sym}. The first k eigenvalues are such that they are very small whereas λ_{k+1} is relatively large. All eigenvalues are ordered increasingly.
3. The number of clusters is set equal to k, according to the eigengap heuristic theory [32].
4. Let $U\in\mathbb{R}^{n\times k}$ be the matrix containing the vectors $\overline{u}_1,\overline{u}_2,\ldots,\overline{u}_k$ as columns. Form the matrix $T\in\mathbb{R}^{n\times k}$ from U by normalizing the rows to norm 1, that is set $t_{ij}=u_{ij}/(\sum_k u_{ik}^2)^{1/2}$.
5. For $i=1,\ldots,n$, let $y_i\in\mathbb{R}^k$be the vector corresponding to the ith row of T.

Fig. 1. The 380 kV Italian power transmission network.

6. Resort to the FKM algorithm [33,34] to partition the data points $(y_i)_{i=1,\ldots,n}$ into k clusters $A_1,\ldots,A_k$.

Output: Clusters $C_1,\ldots,C_k$ with $C_i = j|y_j \in A_i$

In the first step, the Laplacian matrix L_{sym} is calculated from the similarity (affinity) matrix as follows. The input similarity matrix S is of size $n \times n$ and its generic element s_{ij} represents the similarity between nodes i and j in the network. The diagonal components s_{ii} are set to 1 and the matrix is symmetric($s_{ij} = s_{ji}$). The degree matrix D is the diagonal matrix with diagonal entries d_1, d_2,…, d_n defined by

$$d_i = \sum_{j=1}^{N} s_{ij} \quad i = 1,2,\ldots,n. \tag{1}$$

Then, the normalized graph Laplacian matrix can be obtained:

$$L_{sym} = D^{-1/2} L D^{-1/2} = I - D^{-1/2} S D^{-1/2} \tag{2}$$

where $L = D - S$ and I is the identity matrix of size $n \times n$.

It should be noted that the eigengap heuristic theory at the basis of the third step of the algorithm works well when the modularized structure of the data are pronounced whereas the more noisy or overlapping the clusters are, the less effective it is

[32]. In those cases, other methods such as the Markov Clustering Algorithm [35] can be used to find the optimal number of clusters.

2.3. Clustering results and analysis

2.3.1. Affinity construction

As mentioned in the previous section, the result of clustering is sensitive to the similarity function which defines the proximity of the nodes in the network. Since network clustering is to group the vertices of the network into clusters taking into consideration the edge structure of the graph in such a way that there should be many links within each cluster and relatively few between the clusters, using topological information itself is intuitionally appropriate to estimate the structure affinity of node pairs. In this view, two node affinity definitions representative of the local and global topological properties of the network structure are introduced in this paper to support the successive cluster-level criticality analysis.

Possibly, the most straightforward manner to quantify the affinity between a pair of nodes in a network is to use only the local adjacency information: nodes i and j are seen as similar if they are linked directly, otherwise they are not. The consequent adjacency affinity matrix S_1 is identical to the adjacency matrix A of the network.

The adjacency affinity uses only local direct connection information and possibly fails to detect any other structure when a network is not locally dense [24]. Since in this study, we use clustering to decompose the network into topologically dense community structures, for nodes to belong to the same cluster, they should be highly connected to each other, i.e. not necessarily by a direct link but by a short path [36]. For this reason, we introduce the topological distance affinity to drive the clustering. The topological distance (shortest path) d_{ij}between nodes i and j is the minimum number of edges traversed to get from vertex i to vertex j. The matrix D of the topological distances can be extracted from the adjacency matrix A. Thereafter, the topological distance affinity can then be defined based on the elements d_{ij} of D and the Gaussian similarity function:

$$S_2(i,j) = exp(-{d_{ij}}^2/(2\sigma^2)) \;\; i,j = 1,2,\ldots,n \tag{3}$$

where σ is a tuning parameter. This parameter can be tuned to scale the Gaussian similarity function, similarly to the parameter ε in the ε-neighborhood graph [32]. Unfortunately, there are no theoretical results to guide the choice of the parameter, and only some rules of thumb have been suggested in the literature [32]. In our study, we choose a value of 0.8 for σ, which is of the order of the mean distance of a node to its kth nearest neighbor, where k is chosen as $k \sim \log(n)+1$.

Fig. 2 gives out the value landscape of both adjacency affinity matrix S_1 (left) and topological distance affinity matrix S_2 (right) for the 380 kV Italian power transmission network. One can notice the difference in value scale: the adjacency affinity is a sparse matrix with only values 0 and 1, whereas the topological distance affinity measure shows that nodes in local neighborhoods have relatively high similarity value while affinity values between far away nodes are weak, although not necessarily negligible.

2.3.2. Cluster evaluation

The assessment of the quality of the clustering results is a non trivial task because of the unsupervised nature of the analysis. The clustering structure itself and the relational characteristics of the dataset are often utilized as the measurement information for clustering evaluation [25]. In our study, the evaluation of the clustering is based on four representative indices capturing complementary characteristics of the clusters found: the modularity index (Q) as an indicator of the presence of a modularized structure; the Sum of Squared Error (*SSE*) to quantify the cohesion of clusters; the Davies–Bouldin index (*DB*) and Dunn index (*Dunn*) to evaluate high intra-cluster similarity and low inter-cluster similarity, with different metrics.

2.3.2.1. Modularity index. The modularity index Q, introduced by Newman and Girvan [37], attempts to measure how well a given partition of a network compartmentalizes its communities and is defined as [38]:

$$Q = \sum_{i=1}^{k} \left(\frac{e_i}{m} - \left(\frac{\varphi_i}{2m} \right)^2 \right) \tag{4}$$

where k is the number of clusters, e_i defines the number of links in cluster i, φ_i is the sum of the degrees of the nodes in cluster i, and m represents the total number of links in the whole network. Note that when $Q=0$, all the nodes are in one single community while $Q>0$ indicates the existence of some kind of inherent cluster structure. Modularity measures the difference between the total fraction of edges that fall within clusters versus the fraction one would expect if edges were placed at random. Thus, high values of Q represent network partitions in which more of the edges fall within clusters than expected by chance [39]. Moreover, Newman and Girvan [37] suggest that values of Q in the range of 0.2–0.7 designate the presence of cluster structures.

2.3.2.2. Sum of squared error (SSE). Sum of squared error (*SSE*) measures the cohesion of clusters without respect to external information, i.e. quantifies how closely related are the elements in a cluster. *SSE* is suitable for comparing two clustering partitions or two clusters [40]. Given two different sets of clusters resulting

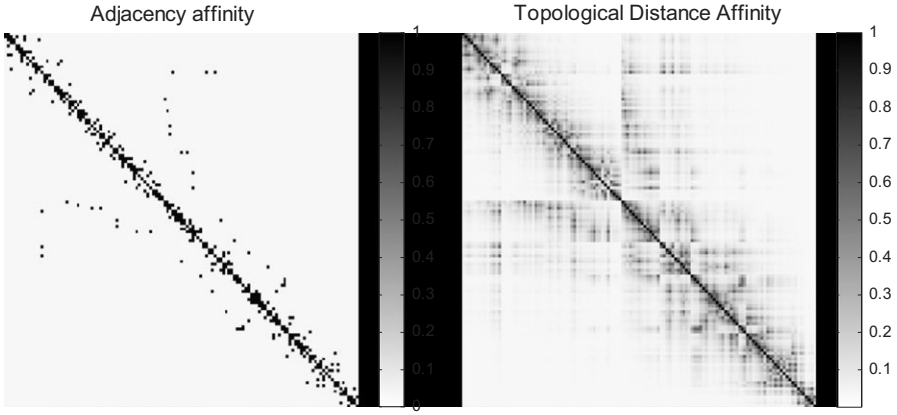


Fig. 2. Adjacency affinity and topological distance affinity matrices for the 380 kV Italian power transmission network.

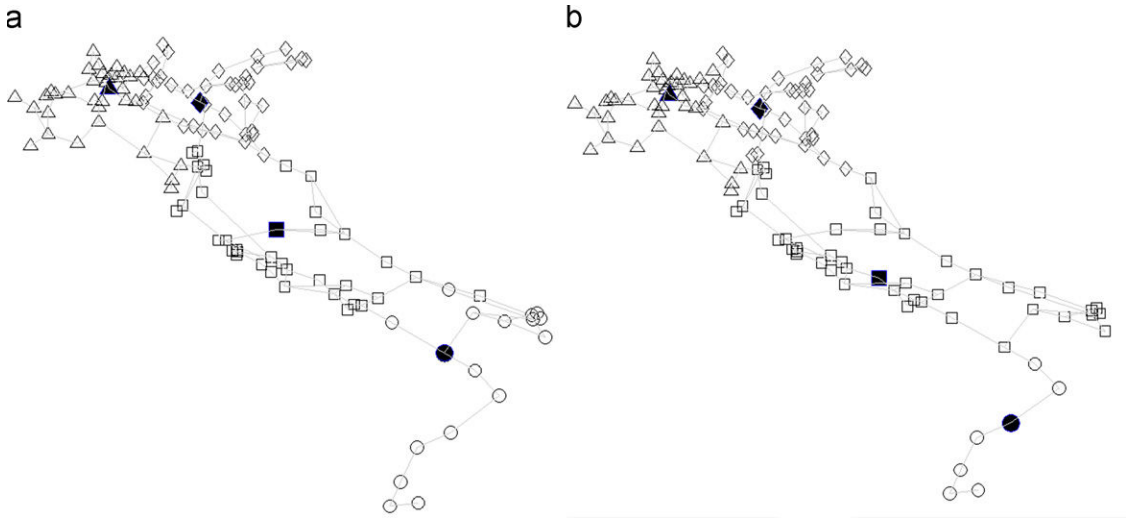


Fig. 3. Clustering results for the adjacency affinity and the topological distance affinity on the 380 kV Italian power transmission network.

from two different clustering procedures, the one with smaller *SSE* is preferable since this means that the prototypes (centroids) of this clustering are superior representations of the points in the clusters. *SSE* is formally defined as follows:

$$SSE = \sum_{i=1}^{k} \sum_{j \in A_i} dist(c_i, j)^2 \tag{5}$$

where *dist* represents the topological distance (shortest path) between node j and the central node c_i of the cluster A_i which node j belongs to.

2.3.2.3. Davies–Bouldin (DB) index [41]. The Davies–Bouldin (*DB*) index introduced in [41] is formulated as follows:

$$DB = (1/k) \sum_{i=1}^{k} \left(\max_{i \neq j} \left\{ \frac{S_i + S_j}{d(c_i, c_j)} \right\} \right) \tag{6}$$

where S_i is the scatter within the ith cluster, i.e. the average distance of all elements in cluster i to its centroid c_i, and $d(c_i,c_j)$ is the distance between clusters i and j. A clustering algorithm that produces a collection of clusters with the smallest Davies–Bouldin index is considered the best algorithm based on this criterion.

2.3.2.4. Dunn index [42]. The *Dunn* index is the ratio of the smallest distance between observations not in the same cluster to the largest intra-cluster distance:

$$Dunn = \min_{1 \le i \le k} \left\{ \min_{1 \le j \le k, j \neq i} \left\{ \frac{\delta(C_i, C_j)}{\max_{1 \le p \le k} \Delta(C_p)} \right\} \right\} \tag{7}$$

where k is the number of clusters, the function δ gives the distance between two clusters C_i and C_j (the shortest path between two centroids) and Δ represents the diameter of a cluster C_p (the maximum shortest path between any node pairs within the cluster). Since internal criterions seek clusters with high intra-cluster similarity and low inter-cluster similarity, algorithms that produce clusters with high *Dunn* index are more desirable.

2.3.3. Clustering analysis of the 380 kV Italian power transmission network

We applied the USCA for performing the clustering analysis of the 380 kV Italian power transmission network. Both adjacency affinity and topological distance affinity were considered. The resulting partitions are showed in Fig. 3(a) and (b), respectively. Different shapes represent different clusters. The filled nodes locate the clusters centers, which are the physical node nearest to the centroids of the clusters based on the Euclidean distance measure. The two different affinity definitions produce somewhat similar partitions in four clusters, though some differences exist. The clusters in both cases exhibit not only physical proximity but also intensity of the relationship in terms of the network connectivity, which results from the fact that generally only nodes with geographical closeness are connected in the power transmission network.

Table 1
Comparison of the clustering results for adjacency affinity and topological distance affinity.

Comparison items	Adjacency affinity	Topological distance affinity
Q	0.664	0.640
Number of cluster	4	4
Cluster central nodes (N_1, N_2, N_3, N_4)	23, 40, 86, 119	23, 40, 99, 121
Cluster size (n_1, n_2, n_3, n_4)	36, 38, 36, 17	36, 41, 43, 7
DB	0.883	0.987
Dunn	0.455	0.455
SSE	1585	1867

Table 1 represents the comparison results of the two partitions. The *Q* values for adjacency affinity and topological distance affinity are both within the range of [0.2, 0.7], which designates the existence of a modularized structure within the 380 kV Italian power transmission network. Partitioning into four clusters is confirmed for both affinities. The size and central node for cluster 1 (whose elements are represented as squares in Fig. 3) are identical and cluster 2 (circles) has same centroid but different size, whereas cluster 3 (triangles) and 4 (diamonds) have neither the same size nor identical central nodes. This discrepancy is probably due to the fact that the nodes in the north part of the Italian transmission network (composed by clusters 1 and 2) are densely connected and their modularized structure is more prominent compared with the south part (composed by clusters 3 and 4), thus both local and global topological affinities can achieve the overall maximum of the modularity. Actually, the *Q* values of the north part of the network (composed by cluster 1 and 2), i.e. 0.443 for adjacency affinity and 0.444 for topological distance affinity, are both higher than those of the south part (composed by clusters 3 and 4), i.e. 0.314 and 0.119 for adjacency affinity and topological distance affinity, respectively.

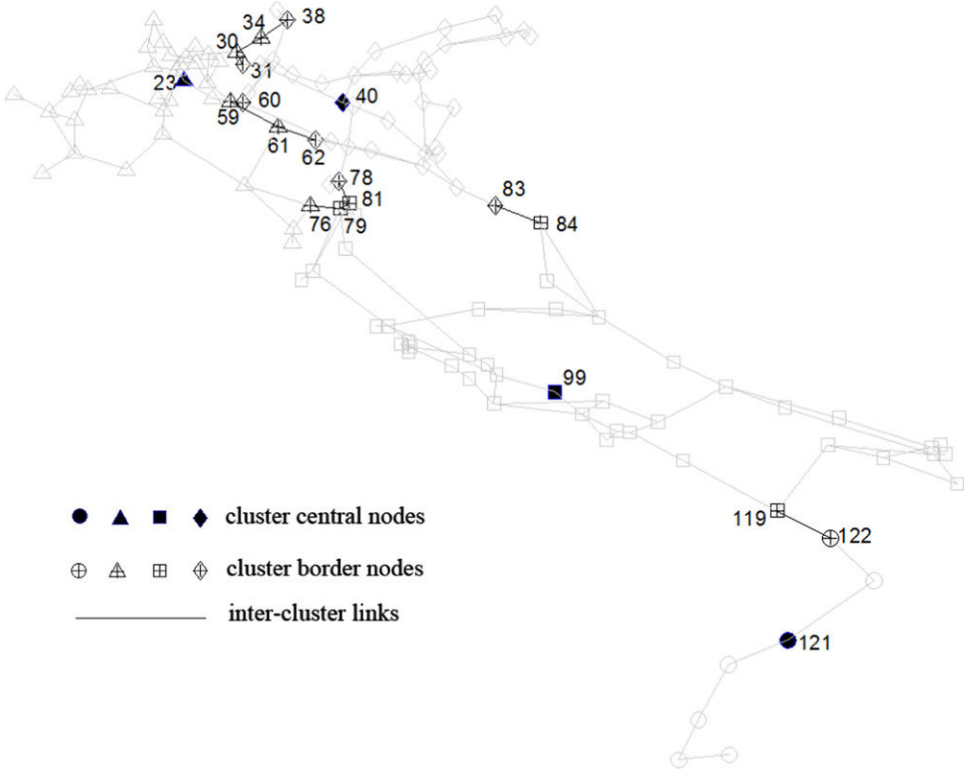


Fig. 4. Inter-cluster links, cluster-border nodes, and central nodes for the 380 kV Italian power transmission network.

In addition, the partitions obtained exhibit $DB=0.883$, $SSE=1585$ for adjacency affinity, and $DB=0.99$, $SSE=1867$ for topological distance affinity. In both evaluation indexes *DB* and *SSE*, clustering by adjacency affinity outperforms that by topological distance affinity. Furthermore, the clusters from adjacency affinity are relatively more balanced in size. For the above reasons, the adjacency affinity is retained for the analyses of the following sections.

2.4. Component importance by clustering

A previous study [11] defined the community-level vulnerability based on the reciprocal of the number of inter-cluster links, thus showing that the modularized structure could be leveraged to the criticality analysis of network elements. In this study, two types of elements in the clustering are paid special attention to (Fig. 4). First, the elements (links and vertices) which are in the periphery and connect different clusters (hereafter called inter-cluster links and cluster-border nodes, respectively) intuitively play a critical role in the complex interaction and communication occurring between different modules of the whole network. In this sense, the so-called overlapping nodes [43,44] are similar to our cluster-border nodes. Second, the central nodes within each cluster, which own highest membership to the cluster, are expected to have a dense pattern of local connections and their failures could possibly propagate to a severe damage to the network.

Fig. 4 represents the inter-cluster links (black lines), cluster-border nodes (nodes with '+' symbol inside) and the central nodes (nodes filled with black color) obtained from the (adjacency affinity) clustering of the 380 kV Italian power transmission network. The inter-cluster links set $E'$is {(30–31), (30–34), (59–60), (61–62), (64–78), (71–83), (76–79), (107–109), (110–111), (112–114)}. Coincidently, the three lines identified as the most critical triplet of lines in [45], because their removal would result in a huge efficiency drop for the whole network, are among the inter-cluster links set E': {(64–78), (71–83), (76–79)}. This shows the importance of these types of elements for the structured robustness of a network, and the usefulness of clustering analysis for their identification.

Table 2
Cluster membership value (MV), rank positions according to the information, degree, closeness, and betweenness centrality measures for cluster-border and central nodes (bold) of each cluster; only the 24 top-ranked are reported.

Cluster	Critical node	MV	Rank C^I	Rank C^D	Rank C^C	Rank C^B
	23	**0.9999**				
	30	0.7296				
1	59	0.7768	13	4	17	8
	61	0.7606	20		9	11
	76	0.5527	15		11	7
	40	**1.0000**			24	18
	31	0.7373				
	34	0.7948				
2	60	0.8699		4	15	22
	62	0.8114			8	
	64	0.8394	5	2	1	4
	71	0.9054	22		14	15
	86	**0.9998**			21	
	78	0.4772	10		6	21
	79	0.9198	8	3	3	5
3	83	0.4775			22	16
	107	0.7442				24
	110	0.8203	10			10
	112	0.5442				
	119	**0.9993**	4			
	109	0.9466				
4	111	0.5724				
	114	0.7314				

Table 2 reports the membership values of these cluster-border nodes and cluster central nodes (bold), and their rank positions according to the information, degree, closeness and betweenness

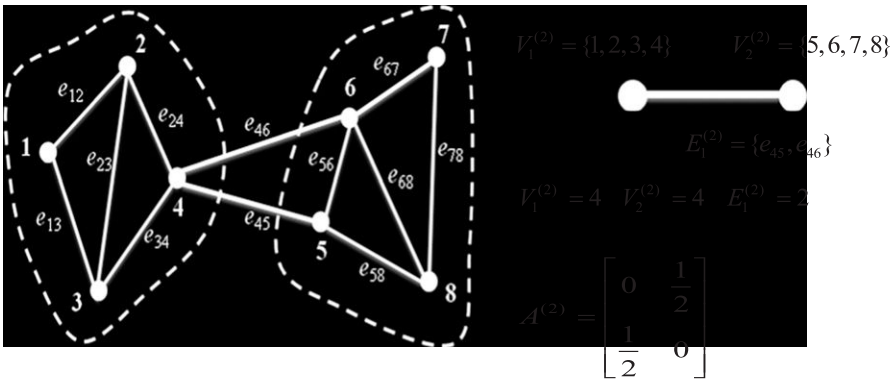


Fig. 5. Illustrative example of the construction of fictitious networks.

centrality measures based on the results in [7]. Detailed definition and explanation of these four centrality measures can be found in the literature [7,15–19]. One can see that most of the nodes found important by clustering, because cluster-border or central, are ranked among the top 24 with highest centrality values, although specific exceptions exist such as the nodes 23, 30, 31, 34, 112 in clusters 1, 2, 3 and the nodes 109, 111 and 114 in cluster 4. This difference is due to the fact that the "clustering-important" nodes are identified based only on regional topological information and not on any other consideration on the role in the whole network.

3. Hierarchical modelling and zoom-in assessment of the network

3.1. Hierarchical model of the network

If one looks closely at the individual clusters in Fig. 3, it may notice that some of them exhibit a modularized structure, and hence can be decomposed further into sub-clusters. Indeed, many real networks reveal a hierarchical organization, where vertices divide into groups that further subdivide into groups of groups, and so forth over multiple scales [4]. On this basis, a framework for hierarchical system modelling has recently been proposed in [25] aiming at reducing the computational burden of modelling the entire system.

For illustration of the potential of the hierarchical modelling framework for complex system analysis, by analogy one may think of the electronic maps such as those provided by Google Maps; the tools are powerful because they present information in a scalable manner—despite the decrease in the amount of information as we "zoom in", the representation shows the information that is relevant at the new scale.

In the same spirit, a hierarchical model representing the whole system at the top and individual elements at the bottom could be obtained via successively performing unsupervised spectral clustering algorithm on the network. Then, based on the hierarchical network representation, fictitious networks can be defined in each level, from which the analyst can extract relevant information at the suitable level of the hierarchy. Fictitious networks are cluster-simplified representations of the real network and can facilitate the understanding and analysis of the network properties by focusing on the relevant information that emerges at the different levels.

Following a similar formulation as in [46], the fictitious network at level k is denoted by a graph$G^{(k)}(\Lambda^{(k)},E^{(k)})$. Let us denote as $V_i^{(k)}(i=1,\ldots,n^{(k)})$ the node i of the fictitious network at level k of the hierarchy and associate a weight to it which is equal to the number of actual nodes which compose $V_i^{(k)}$. These fictitious nodes are connected by $m^{(k)}$ fictitious edges$E^{(k)}=E_1^{(k)},E_2^{(k)},\ldots,E_{m^{(k)}}^{(k)}$. Considering parallel connections, $E_i^{(k)}$ is weighted by the reciprocal of the number of actual edges it contains. Then, the fictitious network is represented by a weighted adjacency matrix $A^{(k)}$whose element $A^{(k)}\left(V_p^{(k)},V_q^{(k)}\right)=1/|E_{pq}^{(k)}|$if the fictitious nodes $V_p^{(k)}$and $V_q^{(k)}$are connected by fictitious edge $E_{pq}^{(k)}$ and 0 otherwise. This definition accounts for the fact that a fictitious edge embracing several real links has that number of paths available between the two communities it connects, thus holding more interaction efficiency and smaller weight viewed as the *physical distance* between the two communities connected by the virtual edge. Fig. 5 gives an example of the construction of a fictitious network.

The 380 kV Italian power transmission network has been modeled as a five levels hierarchy (to which correspond five fictitious networks) by successively applying USCA. In Fig. 6, the weighted fictitious networks and their corresponding weighted adjacency matrices at the levels 2 and 3 of the hierarchy are presented for illustration. The number beside the fictitious node $V_i^{(k)}$represents its weight (number of actual nodes included in the virtual node): for example, the weight of $V_3^{(2)}$ is 36. The fictitious network at level 1 is a single fictitious node whose size is 127, the total number of nodes in the network, whereas at the last level 5 the fictitious network corresponds to the actual physical network.

3.2. Centrality analysis on fictitious networks

Based on the hierarchical representation of the network, problems such as reliability assessment and damage propagation [25] can be swiftly unraveled with low complexity at the expense of low specificity. In this section, we carry out centrality analysis on the fictitious networks, focusing step-wise on the most critical clusters (fictitious nodes) at each scale of the hierarchy. This is valuable for decision makers when they want to allot limited investments to a regional part of the network, which is usually operated by local organizations, to improve the vulnerability of the overall network system.

3.2.1. Efficiency modelling

Network topological efficiency introduced in [46] allows a quantitative analysis of the information flow, and works both in the unweighted abstraction and in the more realistic assumption of weighted networks. This measure is based on the assumption that the information (communication) in a network travels along the shortest routes, and that the efficiency in the communication between two nodes i and j, ε_{ij}, is inversely proportional to their shortest path length d_{ij} which is defined as the smallest sum of the *physical distances* throughout all the possible paths in the

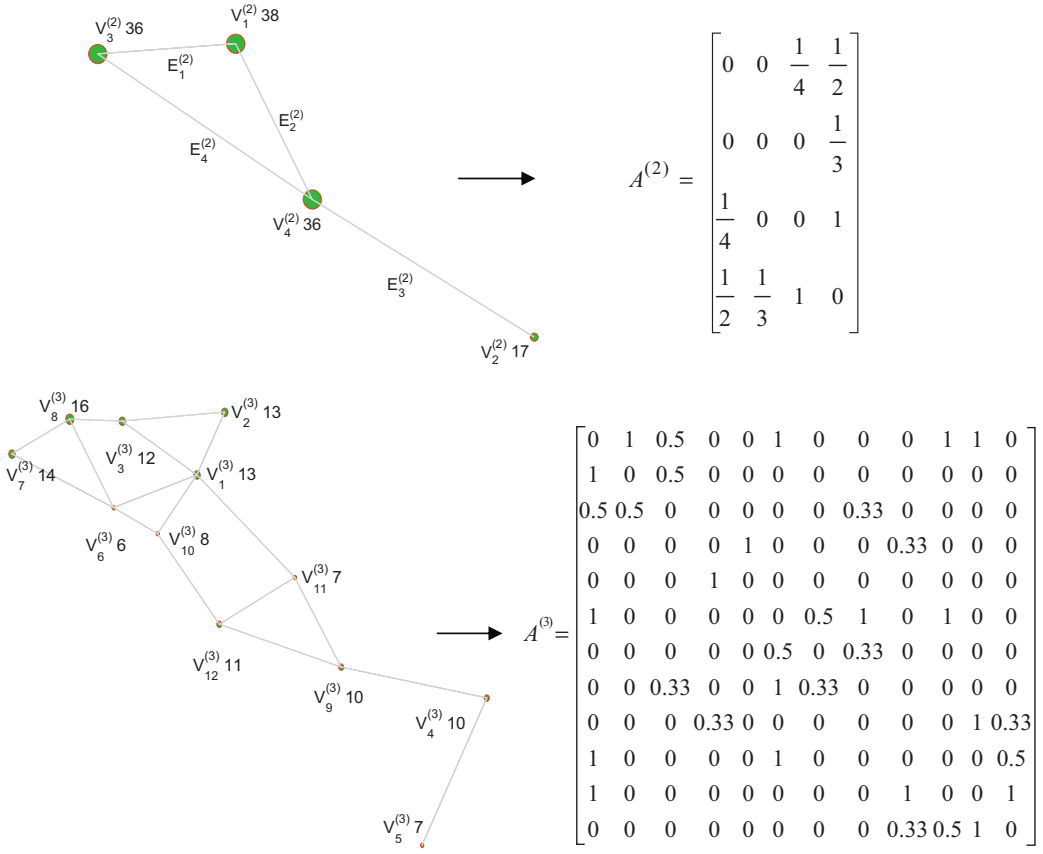


Fig. 6. Fictitious networks and their corresponding weighted adjacency matrices at levels 2 and 3 of the hierarchical model for the 380 kV Italian power transmission network.

weighted network. Then, the efficiency of the whole network is given by:

$$E(G)=\frac{\sum_{i\neq j\in G}\varepsilon_{ij}}{n(n-1)}=\frac{1}{n(n-1)}\sum_{i\neq j\in G}\frac{1}{d_{ij}}. \tag{8}$$

This formula produces a value of E that can vary in the range of $[0,\infty)$.$E(G)$ is defined as 1 in the case of $n=1$, i.e., there is only one single node in the network. It is more practical to have E normalized to be in [0, 1]. For this reason, we consider the ideal case G^{ideal}in which the network has all the $n(n-1)$ possible links among its nodes. In such a case, the information is propagated in the most efficient way since d_{ij} equals the *physical distance* between nodes i and j and E assumes its maximum value. The efficiency $E(G)$ considered in the following of the paper is always divided by $E(G^{ideal})$ and therefore$0\leq E(G)\leq 1$.

Notice that, for our analysis of fictitious networks modelling of the Italian power transmission network, the *physical distance* exists even if there is no fictitious edge between two nodes $V_p^{(k)}$and$V_q^{(k)}$: for generality, their physical distance is defined as the reciprocal of the minimum size of the two fictitious nodes if there is not fictitious edge connecting them. By this definition, the *physical distance* of nodes in the bottom level fictitious network, i.e. the actual network, coincides with that obtained by considering it as an unweighted network.

Fig. 7 plots the efficiency values of the fictitious networks at each level of the hierarchy. It can be observed that as the evaluation moves down in the hierarchy, the efficiency difference between the fictitious network and the actual network decreases as expected. Note that the minimum efficiency at level 3 stems from the fact that the ideal fictitious networks G^{ideal} have different topologies and link weights at different levels of the hierarchy.

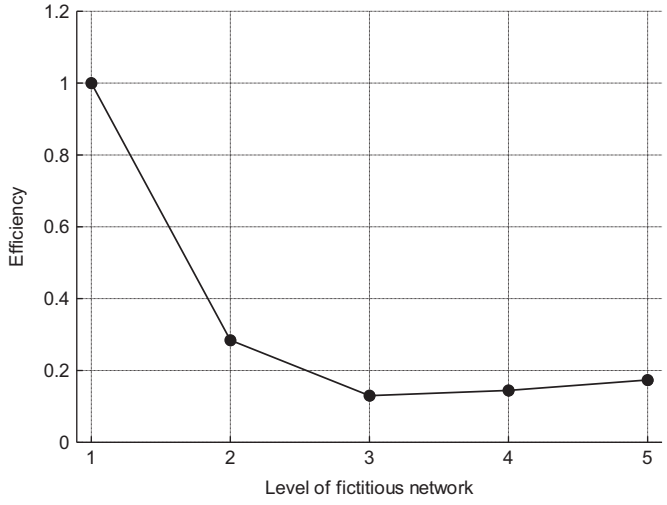


Fig. 7. Network efficiency of fictitious networks at each level of the hierarchy.

Thus, it is not necessary that the curve of network efficiency decreases monotonically. Fig. 7 is used to qualitatively show that as the evaluation moves down in the hierarchy, the efficiency approximation gets closer to the efficiency of the actual network.

3.2.2. *Zoom-in criticality analysis*

The hierarchical model makes a multi-scale criticality analysis possible, beyond the widely studied component-level criticality analysis. This zoom-in criticality analysis is analogous to the procedure of locating a specific site in a scalable electronic map

manually: a large area is first fixed at the coarse granular scale of the map based on the limited information at that level, and then the user can zoom in on that area to get a relatively fine-grained view which offers more local information, based on which a narrower region can be identified, repeating this operation until the desired scale of the map.

Information centrality is used as an illustration to quantify the importance criticality of a cluster on the network. Parallel with the component information centrality definition [18,19,47], we define the information centrality for cluster $V_i^{(k)}$ at level k of the hierarchy as the information centrality of its corresponding fictitious node in the fictitious networks, i.e. the relative drop in the fictitious network topological efficiency caused by the removal of all the fictitious edges incident in $V_i^{(k)}$:

$$C^I_{V_i^{(k)}} = \frac{\Delta E(V_i^{(k)})}{E} = \frac{E[G^{(k)}] - E[G_r^{(k)}]}{E[G^{(k)}]} \tag{9}$$

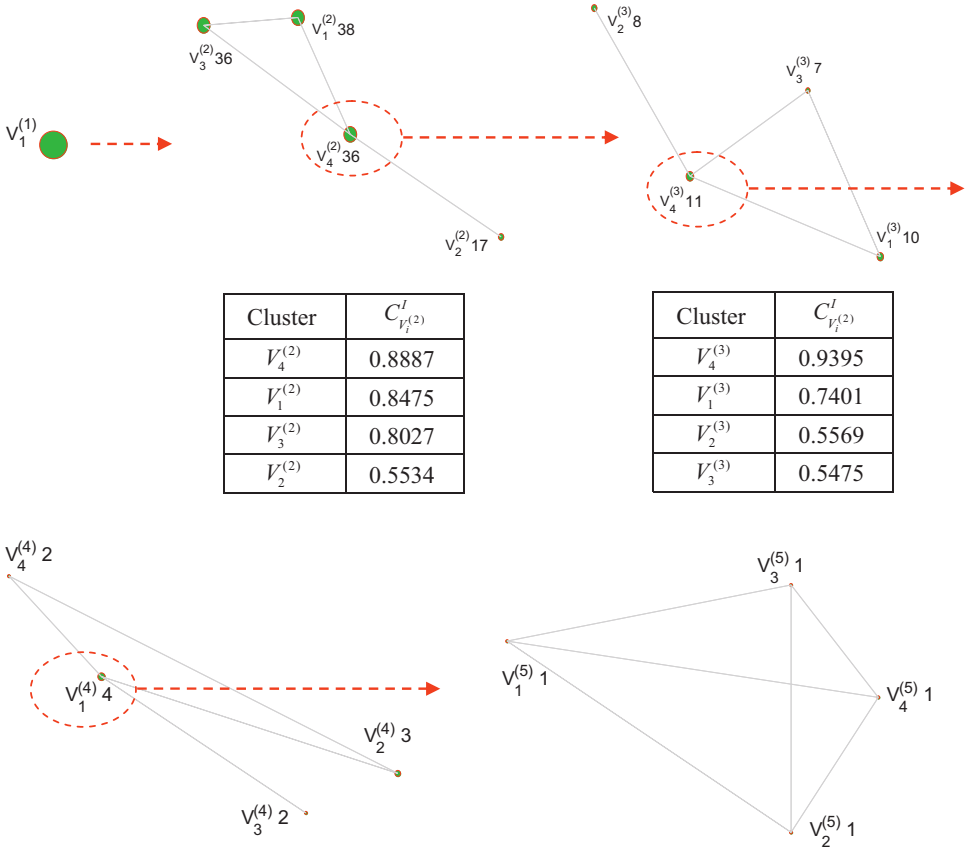
where $G_r^{(k)}$ is the network obtained by removing from the original fictitious network the fictitious edges incident in node $V_i^{(k)}$.

An illustration of the process of zoom-in criticality analysis on the 5-levels hierarchical model of the 380 kV Italian power transmission network built by clustering in Section 3.1 is presented in Fig. 8. By first 'opening' the single unit at level 1, a weighted fictitious network with 4 nodes at level 2 is achieved, in which the information centrality of each fictitious node is calculated according to Eq. (9) and is presented in the corresponding Table. It shows that node $V_4^{(2)}$ owns the highest C^I value; then, the internal topology of $V_4^{(2)}$ at level 3 of the hierarchy is unraveled by zooming into $V_4^{(2)}$. Similarly, the most critical clusters at levels 3 and 4 can be determined as $V_4^{(3)}$ and $V_1^{(4)}$, which include 11 and 4 actual nodes, respectively. In level 5, which represents the real network, however, the four nodes have the same values of information centrality since they are completely connected and the removal of all the edges incident in any one of the four nodes would result in the equal relative drop in the network topological efficiency.

Note that the difference of cluster-level information centrality is quite pronounced for the 380 kV Italian power transmission network, compared to the node-level information centrality reported in [7] where the difference between the biggest and smallest C^I values is only 0.0194; then, the analyst may have more confidence to make clear-cut, relevant decisions based on the cluster-level criticality results of the 380 kV Italian power transmission network.

4. Conclusions

In this article, the feasibility of extracting cluster-level structural properties for a realistic-size network by clustering analysis



Cluster	$C^I_{V_i^{(2)}}$
$V_4^{(2)}$	0.8887
$V_1^{(2)}$	0.8475
$V_3^{(2)}$	0.8027
$V_2^{(2)}$	0.5534

Cluster	$C^I_{V_i^{(2)}}$
$V_4^{(3)}$	0.9395
$V_1^{(3)}$	0.7401
$V_2^{(3)}$	0.5569
$V_3^{(3)}$	0.5475

Cluster	$C^I_{V_i^{(4)}}$
$V_1^{(4)}$	0.8667
$V_2^{(4)}$	0.6364
$V_4^{(4)}$	0.6000
$V_3^{(4)}$	0.4667

Cluster	Nodes	$C^I_{V_i^{(5)}}$
$V_1^{(5)}$	89	0.50
$V_2^{(5)}$	90	0.50
$V_3^{(5)}$	91	0.50
$V_4^{(5)}$	92	0.50

Fig. 8. The process of zooming-in analysis of information centrality in the hierarchy.

has been first investigated, taking as reference example the 380 kV Italian power transmission network structure. Then, the hierarchical modelling framework has been utilized to represent the networked system, forming a scalable hierarchical structure of corresponding fictitious networks. In the context of the hierarchical representation of the network, zoom-in criticality analysis has been proposed to identify the most relevant clusters at the desired level of the hierarchy.

For clustering analysis, both adjacency affinity and topological affinity have been considered when applying USCA on the 380 kV Italian power transmission network structure, and their results have been compared to those of four classic centrality measures. For the considered network, the adjacency affinity has turned out to give superior partition. Also, the inter-cluster links, cluster-border nodes and central nodes of each cluster, have been identified as critical: most of the nodes found important by clustering, because cluster-border or central, have turned out to be ranked among the top 24 with highest centrality values (*CI*, *CD*, *CC* and *CB*) and the most critical triplet of lines identified in [45] is contained within the inter-cluster links set. This confirms the importance of these types of elements for the structural robustness of a network and the usefulness of clustering analysis for their identification.

Then, the systemic hierarchical representation has been introduced for modelling and analysis of complex network systems, with the objective of rendering more manageable the treatment of real-world critical infrastructures. A five-level hierarchical model of the 380 kV Italian power transmission network structure has been obtained by successively applying USCA. The cluster-level information centrality has been proposed and used as an illustration to quantify the importance criticality of a cluster in the network. The most critical clusters at each level of the hierarchy have been identified with high confidence for decision making.

Finally, a comment is in order with respect to the computational complexity of the approach proposed. The complexity depends primarily on the computational cost of spectral clustering, where a large number of eigenvectors have to be computed for large graph Laplace matrices (step 2 of the algorithm), whose time complexity of computing eigenvectors is $O(n^3)$[48]. Thus, the computation cost of constructing the hierarchical model is$O(n^3 l)$, where l is the number of hierarchical levels. In general, the high-quality clustering of the spectral method is at the expense of its comparatively demanding computation cost. In this study, the spectral clustering is adopted as one possible way to extract some inherent cluster-level structural properties and derive the hierarchical modelling which sets the base for a multi-scale criticality analysis, which is our main objective. Furthermore, as many real adjacency matrices are sparse in nature, efficient existing methods to compute the eigenvectors of sparse matrices need to be adopted [49]. Finally, some improvements of spectral clustering have been proposed in Statistics and Data Mining such as parallel spectral clustering [50], distributed method [51] and fast approximation [52] to make it scalable to large network problems.

Acknowledgements

The authors are thankful to Dr. Giovanni Sansavini of Politecnico di Milano for supporting the work with relevant information on the network structure uses as reference system and to Dr. Franck Marle for fruitful discussions.

References

[1] Ellis J, Fisher D, et al. Report to the President's Commission on critical infrastructure protection. S. E. Institute, Editor Carnegie Mellon University, 1997.
[2] Wasserman S, Faust K. Social network analysis. Cambridge: Cambridge University Press; 1994.
[3] Albert R, Barabasi A-L. Statistical mechanics of complex networks. Reviews of Modern Physics 2002;74:47–97.
[4] Clauset A, Moore C, Newman MEJ. Hierarchical structure and the prediction of missing links in networks. Nature 2008;453:98–101.
[5] Fortunato S. Community detection in graphs. Physics Reports 2010;486 (75):174.
[6] Scott J. Social network analysis: a handbook. 2nd ed. London: Sage; 2000.
[7] Zio E, Sansavini G. Component criticality in failure cascade processes of network systems. Risk Analysis 2011;31:1196–210.
[8] Zio E, Golea LR, Rocco CM. S. Identifying groups of critical edges in a realistic electrical network by multi-objective genetic algorithms. Reliability Engineering and System Safety 2012;99:172–7.
[9] Zio E. From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures. International Journal of Critical Infrastructures 2007;3(3):488–508.
[10] Yazdani, A, P Jeffrey. A note on measurement of network vulnerability under random and intentional attacks. arXiv:1006.2791v1 [physics.comp-ph] 14 Jun 2010.
[11] Rocco S, Claudio M, Ramirez-Marquez José Emmanuel. Vulnerability metrics and analysis for communities in complex networks. Reliability Engineering & System Safety 2011;96(10):1360–6.
[12] Latora V, Marchiori M. Economic small-world behavior in weighted networks. European Physical Journal B: Condensed Matter and Complex Systems 2003;32:249–63.
[13] Criado, R, J Flores, A Garcıa del Amo, J Pello, M Romance, M Vela-Pérez. Understanding complex networks through the study of their critical nodes: efficiency, vulnerability and dynamical importance. In: Proceedings of the 2007 international conference on modelling and computation on complex networks and related topics Net-Works 2007 Aranjuez, Spain, 2007.
[14] Criado, R, J Pello, M Romance, M Vela-Pérez. Structural analysis and optimality of vulnerability and efficiency in artificial networks. In: Proceedings of the 2007 international conference on modelling and computation on complex networks and related topics Net-Works 2007 Aranjuez, Spain, 2007.
[15] Sabidussi G. The centrality index of graphs. Psychometrika 1966;31(4): 581–603.
[16] Nieminen J. On the centrality in a graph. Scandinavian Journal of Psychology 1974;15(1):332–6.
[17] Freeman LC. Centrality in social networks conceptual clarification. Social Networks 1978;1(3):215–39.
[18] Latora V, Marchiori M. A measure of centrality based on the network efficiency. New Journal of Physics 2007;9:188 (12 pages).
[19] Little RG. Controlling cascading failure: understanding the vulnerabilities of interconnected infrastructures. Journal of Urban Technology 2002;9(1):109–23.
[20] Mason A, Onnela J, Mucha P. Communities in networks. Notices of the American Mathematical Society 2009;56:9.
[21] Karrer B, Levina E, Newman M. Robustness of community structure in networks. Physical Review E: Statistical, Nonlinear, and Soft Matter Physics 2008;77:046119.
[22] Eum S, Arakawa S, Murata M. Traffic dynamic in modularity structure of complex networks. In: Proceedings of the fifth international conference on broadband communications, networks and systems, 2008. BROADNETS2008. Issue Date: 8–11Sept; 2008, p. 390–395.
[23] Wu J, Gao Z, Sun H. Cascade and breakdown in scale-free networks with community structure. Physical Review E: Statistical, Nonlinear, and Soft Matter Physics 2006;74:066111.
[24] Sales-Pardo M, Guimerá R, Moreira A A, Moreira, Amaral LAN. Extracting the hierarchical organization of complex systems. Proceedings of the National academy of Sciences of the United States of America 2007;104:15224–9.
[25] Gómez C, Sánchez-Silva M, Duenas-Osorio L. (2011). Clustering methods for risk assessment of infrastructure network systems. Applications of statistics and probability in Civil Engineering. Faber, Köhler and Nishijima (Eds). ISBN:978-0-415-66986-3.
[26] Brandes U, Erlebach T. Network analysis: methodological foundations. LNCS. Berlin: Springer; 2005 3418.
[27] Rosato V, Bologna S, Tiriticco F. Topological properties of high-voltage electrical transmission networks. Electric Power Systems Research 2007;77: 99–105.
[28] Filippone M, Camastra F, Masulli F, Rovetta S. A survey of kernel and spectral methods for clustering. Pattern Recognition 2008;41(1):176–90.
[29] Scholkopf B, Smola AJ, Muller KR. Nonlinear component analysis as a kernel eigenvalue problem. Neural Computation 1998;10(5):1299–319.
[30] Jain A K, Murty MN, Flynn PJ. Data clustering: a review. ACM Computing Surveys (CSUR) 1999;31(3):264–323.
[31] Schaeffer SE. Graph clustering. Computer Science Review 2007;1(1):27–64.
[32] Von Luxburg Ulrike. A tutorial on spectral clustering. Statistics and Computing 17.4 2007:395–416.
[33] Leguizamon S, HP, Azzali S. Unsupervised Fuzzy *C*-means classification for the determination of dynamically homogeneous areas. p. 851-856, 1996.
[34] Alata M, Molhim M, Ramini A. Optimizing of Fuzzy *C*-means clustering algorithm using GA. World Academy of Science, Engineering and Technology 2008:224–9.
[35] van Dongen, Stijn Marinus. Graph clustering by flow simulation. (2000).
[36] Edachery, Jubin, Arunabha Sen, Franz Brandenburg. Graph clustering using distance-*k* cliques. In: Graph drawing, pp. 98–106. Springer Berlin/Heidelberg; 1999.

[37] Newman M, Girvan M. Finding and evaluating community structure in networks. Physical Review E: Statistical, Nonlinear, and Soft Matter Physics 2004;69(2):026113.
[38] Good B, de Montjoye Y, Clauset A. The performance of modularity maximization in practical contexts. Physical Review E: Statistical, Nonlinear, and Soft Matter Physics 2010;81:046106.
[39] Mason A, Onnela J, Mucha P. Communities in networks. Notices of the American Mathematical Society 2009;56:9.
[40] Tan P-N, Steinbach M, Kumar V. Introduction to data mining: chapter 8 cluster analysis—basic concepts and algorithms. Addison-Wesley; 2005.
[41] Davies DL, Bouldin DW. A cluster separation measure. IEEE Transactions on Pattern Analysis and Machine Intelligence 1979;2:224.
[42] Dunn JC. A Fuzzy relative of the ISODATA process and its use in detecting compact well-separated clusters. Journal of Cybernetics 1973;3(3):32–57.
[43] Lázár A, Ábel D, Vicsek T. Modularity measure of networks with overlapping communities. 2010 EPL 90 18001.
[44] Gregory Steve. Fuzzy overlapping communities in networks. Journal of Statistical Mechanics: Theory and Experiment 2011 ISSN:1742-5468, pp. P02017. February.
[45] Crucitti P, Latora V, Marchiori M. Locating critical lines in high-voltage electrical power grids. Fluctuations and Noise Letters 2005;5(2):L201–8.
[46] Latora V, Marchiori M. Efficient behavior of small-world networks. Physical Review Letters 2001;87:198701.
[47] Latora V, Marchiori M. Vulnerability and protection of infrastructure networks. Physical Review E: Statistical, Nonlinear, and Soft Matter Physics 2005;71(1):015103.
[48] Schaeffer, Satu Elisa. Graph clustering. Computer Science Review 2007;1(1):27–64.
[49] Golub G, Van Loan D. Matrix computations. Baltimore: Johns Hopkins University Press; 1996.
[50] Song Yangqiu, Wen-Yen Chen, Hongjie Bai, Chih-Jen Lin, Chang Edward. Parallel spectral clustering. Machine Learning and Knowledge Discovery in Databases 2008:374–89.
[51] Kempe David, Frank McSherry. A decentralized algorithm for spectral analysis. Journal of Computer and System Sciences 2008;74(1):70–83.
[52] Yan, Donghui, Ling Huang, Michael I. Jordan. Fast approximate spectral clustering. In Proceedings of the 15th ACM SIGKDD international conference on knowledge discovery and data mining, pp. 907–916. ACM; 2009.

Paper [2] Y.-P. Fang, E. Zio. "Hierarchical Modelling by Recursive Unsupervised Spectral Clustering and Network Extended Importance Measures to Analyze the Reliability Characteristics of Complex Network Systems." American Journal of Operation Research, 3(1A): 101-112, 2013.

American Journal of Operations Research, **2013, 3, 101-112**
doi:10.4236/ajor.2013.31A010 Published Online January 2013 (http://www.scirp.org/journal/ajor)

Hierarchical Modeling by Recursive Unsupervised Spectral Clustering and Network Extended Importance Measures to Analyze the Reliability Characteristics of Complex Network Systems

Yiping Fang[1], Enrico Zio[1,2]
[1]Chair on Systems Science and the Energetic Challenge, Ecole Centrale Paris and Supelec, Paris, France
[2]Energy Department, Politecnico di Milano, Milano, Italy
Email: yiping.fang@ecp.fr

Received November 30, 2012; revised December 30, 2012; accepted January 13, 2013

ABSTRACT

The complexity of large-scale network systems made of a large number of nonlinearly interconnected components is a restrictive facet for their modeling and analysis. In this paper, we propose a framework of hierarchical modeling of a complex network system, based on a recursive unsupervised spectral clustering method. The hierarchical model serves the purpose of facilitating the management of complexity in the analysis of real-world critical infrastructures. We exemplify this by referring to the reliability analysis of the 380 kV Italian Power Transmission Network (IPTN). In this work of analysis, the classical component Importance Measures (IMs) of reliability theory have been extended to render them compatible and applicable to a complex distributed network system. By utilizing these extended IMs, the reliability properties of the IPTN system can be evaluated in the framework of the hierarchical system model, with the aim of providing risk managers with information on the risk/safety significance of system structures and components.

Keywords: Complex Network System; Hierarchical Modeling; Spectral Clustering; Extended Importance Measure

1. Introduction

Critical infrastructures are engineered distributed systems which provide the fundamental support to modern Industry and society. Examples are computer and communication systems, power transmission and distribution systems, rail and road transportation systems, oil/gas systems and water distribution systems. Failures of such systems can have multiple, transnational impacts of significant size [1-3]. Hence, identifying and quantifying the reliability and vulnerability of such systems is crucial for designing the adequate protections, mitigation and emergency actions against failures [2].

These systems are exposed to multiple hazards and threats, some of which are even unexpected and emergent, and consist of a large number of elements whose interactions are not easily modeled and quantified, so that a complete analysis by exhaustive treatment cannot be pursued. As a result, the performance and reliability assessment of such 'complex' systems has proved to be a non-trivial task in practice.

Recent studies suggest that many real complex network systems exhibit a modularized organization [4,5]. In many cases, these modularized structures are found to correspond to functional units within networks (ecological niches in food webs, modules in biochemical networks) [6]. Broadly speaking, clusters (also called communities or modules) are found in the network, forming groups of elements that are densely interconnected with each other but only sparsely connected with the rest of the network. Furthermore, hierarchically modularized organization, which is a central idea for the life process in biology [5,7], is also found to characterize the internal structure of many technological networks [8]. This sparks the idea of utilizing the hierarchical, modularized structure as a basis to model these complex systems, for their analysis and understanding [9].

In the analysis of systems with respect to their failure behavior, Importance Measures (IMs) are used to identify the weak points and quantify the impact of component failures [10,11]. IMs provide numerical indicators to determine which components are most important for system reliability improvement or most critical for system failure. Many different IMs have been proposed in the literature [12,13], among which classical and relevant statistics are Birnbaum [14], Fussell-Vesely [15] and Criticality Importance [16,17]. However, none of these

Figure 1. The 380 kV Italian power transmission network.

measures can be applied directly to complex network systems, because of the distributed character of functionality and service that they provide.

The purpose of this paper is twofold: firstly to propose a scheme of recursive clustering to obtain a hierarchical modeling framework associated with different varied-size grained virtual networks; then to introduce Extended Importance Measures (EIMs) which are compatible with the distributed characteristics of complex network systems, to evaluate the components importance in the framework of the hierarchical system representation.

The remainder of this paper is organized as follows:

Section 2 presents the methodology of hierarchical modeling, taking the structure of the 380kV Italian Power Transmission Network (IPTN) as an example for illustration; in Section 3, the basic terminal-pair connection reliability problem is first introduced, based on which the traditional IMs are extended and then calculated for the IPTN system; conclusions are drawn in Section 4.

2. Hierarchical Modeling of Complex Network System

2.1. Network Representation

Graph Theory provides a framework for the mathematical representation of complex networks. A graph is an ordered pair $G(V,E)$ comprising a set of vertices (nodes) $V=\{v_1,v_2,\cdots,v_N\}$ together with a set of edges (also called arcs or links) $E=\{e_1,e_2,\cdots,e_M\}$, which are two-element subsets of *V*. The network structure is usually defined by the $N\times N$ *adjacency matrix*, which defines which two nodes are connected by assigning a 1 to the corresponding element of the matrix; otherwise, the value in the matrix is 0 if there is no connection between the two nodes. As described, this type of graph is unweighted and undirected. A graph is weighted if a value (weight) is assigned to each edge representing properties of the connection like cost, reliability, capacities, etc. For example, the *matrix of physical distances* is often used in conjunction with the *adjacency matrix* to describe a network also with respect to its spatial dimension [18,19].

In this paper, we take for exemplification of the analyses proposed the 380 kV Italian power transmission network (IPTN) (**Figure 1**). This network is a branch of the high-voltage-level transmission network, which can be modeled as a graph of $N=127$nodes ($N_G=30$ generators and $N_D=97$ distributors) connected by *M* = 171 links [20,21], defined by its $N\times N$ adjacency matrix *A* whose entries $\left[a_{ij}\right]$ are 1 if there is an edge joining node *i* to node *j* or 0 otherwise. In **Figure 1**, the generators, *i.e*. hydro and thermal power plants, are represented by squares whereas the distribution substations are represented by circles.

2.2. Construct Network Hierarchy by Successive Clustering

Modularity is ubiquitous in many networks of scientific and technological interest, ranging from the World Wide Web to biological networks [7,22]. As a result, it is often possible to identify groups of elements that are highly interconnected with each other, but have only a few links to components outside of the group to which they belong to. These communities usually combine into each other in a hierarchical manner [7], in which nodes form groups and then join the groups of groups, and so forth, starting from the lowest levels of organization (individual nodes) up to the level of the entire system. This suggests the development of a hierarchical structure to describe a complex network system at different levels of resolution, with the aim of managing the complexity of the system more effectively.

A successive Unsupervised Spectral Clustering Algorithm (USCA) [23], which is invariant to cluster shapes and densities and simple to implement, has been adopted in this study to build the hierarchical structure of the IPTN system. Cluster analysis aims at recognizing natural groups within classes of entities [24]. The problem is to assign categories to unlabelled data, encouraging the search of implicit information in the network structure encoded in its graph [25]. Consequently, modularity patterns within a complex network system can be revealed without a priori knowledge of their existence. The detailed description of different clustering methods is beyond the scope of this article. For a systematic and synthetic review, the reader is encouraged to look at [24-26].

The USCA makes use of the spectrum (eigenvalues) of the similarity matrix of the data to perform dimensionality reduction before Fuzzy c-Means (FCM)—clustering in fewer dimensions. Schematically, it is performed by the steps [23] in **Table 1**.

In the first step, the Laplacian matrix L_{sym} is calculated from the similarity (affinity) matrix as follows. The input similarity matrix *S* is of size $n\times n$ and its generic element s_{ij} represents the similarity between nodes *i* and *j* in the network. The diagonal components s_{ii} are set to 1 and the matrix is symmetric $\left(s_{ij}=s_{ji}\right)$. The degree matrix D is the diagonal matrix with diagonal entries $d_1,d_2,\cdots,d_n$ defined by

$$d_i=\sum_{j=1}^{N}s_{ij},i=1,2,\cdots,n \tag{1}$$

Then, the normalized graph Laplacian matrix can be obtained:

$$L_{sym}=D^{-1/2}LD^{-1/2}=I-D^{-1/2}SD^{-1/2} \tag{2}$$

where $L=D-S$ and I is the identity matrix of size $n\times n$.

By recursively operating the USCA on the data of the IPTN presented in Section 2.1 above, a 5-levels hierarchical structure of the system is constructed which contains the complete system at the top and individual elements at the bottom (the top panel of **Figure 2** gives out the structure of the hierarchy, detailed in the first 3 levels).

2.3. Hierarchical Modeling of the Network

Based on the hierarchy structure resulting from the successive application of USCA, artificial networks can be

Table 1. Unsupervised spectral clustering algorithm.

Input: Similarity matrix $S \in \mathbb{R}^{n\times n}$.
Compute the normalized graph Laplacian matrix L_{sym}.
Compute the first k eigenvalues $\lambda_1,\lambda_2,\cdots,\lambda_k$ and corresponding eigenvectors $\bar{u}_1,\bar{u}_2,\cdots,\bar{u}_k$ of matrix L_{sym}. The first k eigenvalues are such that they are very small whereas λ_{k+1} is relatively large.
The number of clusters c is set equal to k, according to the eigengap heuristic theory [24].
Let $U \in \mathbb{R}^{n\times k}$ be the matrix containing the vectors $\bar{u}_1,\bar{u}_2,\cdots,\bar{u}_k$ as columns. Form the matrix $T \in \mathbb{R}^{n\times k}$ from U by normalizing the rows to norm 1, that is set $t_{ij} = u_{ij} \Big/ \left(\sum_k u_{ik}^2\right)^{1/2}$.
For $i = 1,\cdots,n$ let $y_i \in \mathbb{R}^k$ be the vector corresponding to the i-th row of T.
Resort to the FCM algorithm [27,28] to partition the data points $(y_i)_{i=1,\cdots,n}$ into $c = k$ clusters $C_1,\cdots,C_k$.
Output: Clusters $A_1,\cdots,A_k$ with $A_i = \{j \mid y_j \in C_i\}$

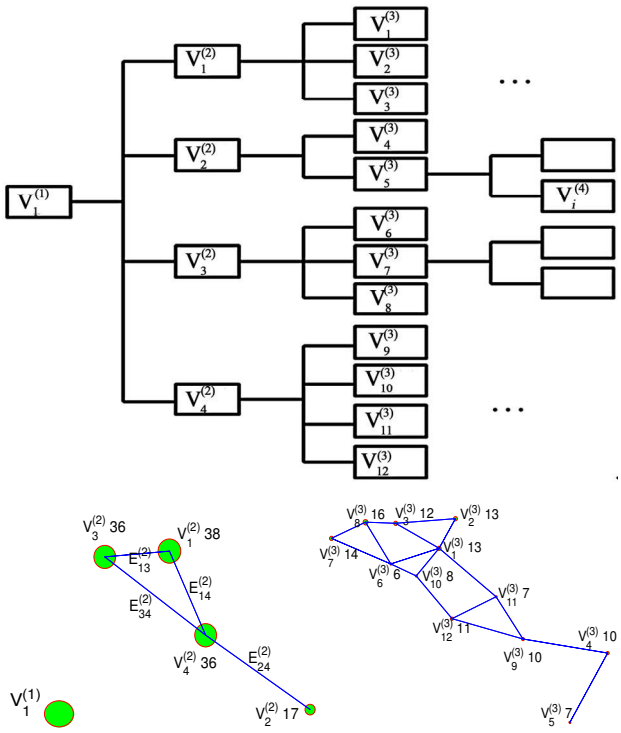


Figure 2. The hierarchy structure of the IPTN system and associated artificial networks of the first three levels.

defined at each layer. The artificial network at level l of the hierarchy is described as a graph $G^{(l)}\left(\Lambda^{(l)}, E^{(l)}\right)$ with $1 \le l \le L$, where L is the number of levels of the hierarchy. We use $V_i^{(l)}$ to represent the artificial node i $\left(\text{for } i = 1,2,\cdots,\left|\Lambda^{(l)}\right|\right)$ at level l, which corresponds to a cluster of real network nodes. Artificial nodes are connected by artificial links

$$E_{ij}^{(l)}\left(\text{for } i = 1,2,\cdots,\left|\Lambda^{(l)}\right| \text{ and } i \ne j\right),$$

composed by those actual network links connecting (in parallel) the actual nodes in the clusters forming the artificial nodes,

$$E_{ij}^{(l)} = \left\{e_{st} \middle| v_s \in V_i^{(l)}, v_t \in V_j^{(l)}\right\}.$$

The connection pattern between artificial nodes at level l is illustrated by an *adjacency matrix* $A^{(l)}$ whose element

$$A^{(l)}\left(V_i^{(l)}, V_j^{(l)}\right) = 1 \quad \text{if} \quad E_{ij}^{(l)} \ne \varnothing,$$

i.e. if in the artificial nodes $V_i^{(l)}$ and $V_j^{(l)}$ there is at least one actual link connecting two actual nodes, and 0 otherwise.

Figure 2 presents the hierarchy structure of the IPTN system and the artificial networks associated with the first 3 levels of the hierarchy. At the top of the hierarchy (*i.e.* $l = 1$), the network is a single unit, *i.e.* one artificial node $V_1^{(1)}$, which consist of all actual nodes. At the second level $(l = 2)$, we have

$$\Lambda^{(2)} = \left\{V_1^{(2)}, V_2^{(2)}, V_3^{(2)}, V_4^{(2)}\right\}$$

and $E^{(2)} = \left\{E_{13}^{(2)}, E_{14}^{(2)}, E_{34}^{(2)}, E_{24}^{(2)}\right\}$

with $V_1^{(2)}, V_2^{(2)}, V_3^{(2)}, V_4^{(2)} \subset V_1^{(1)}$.

The integer that is indicated in the Figure in proximity of the generic i-th artificial node $V_i^{(2)}$ indicates the number of actual nodes which compose it, e.g. $V_1^{(2)}$ is representative of a group of 38 actual network nodes. Note that at the bottom of the hierarchy, we find the original network, *i.e.* each artificial node is an actual node and each artificial edge corresponds to an actual link.

The hierarchical model offers different levels of resolution at the different levels of the hierarchy. The artificial networks at the top of the hierarchy contain limited detail information of the local connectivity patterns (in the limit, only one node represents the whole network at the first level of the hierarchy); as we move down the hierarchy, more local information enters the model, at the expense of an increase in the dimension of the network. These characteristics can be leveraged efficiently to manage the complexity of a complex network system.

3. Reliability Analysis Based on the Hierarchical Model

It is known that most network reliability problems are *NP*-hard and therefore there is a significant gap between theoretical analysis and the ability to compute different

reliability parameters for large or even moderate network systems [11]. In this respect, hierarchical modeling sets up a framework based on which reliability and vulnerability characteristics of complex network systems can be computed efficiently, thanks to the multi-scaled information representation scheme.

3.1. Terminal-Pairs Reliability Assessment

The terminal-pair or node-pair reliability (TPR) problem amounts to determining the probability of successful communication between a specified source node and a terminal node in a network, given the probability of success of each link and node in the network. Let us introduce a binary vector $S_k = \{x_1, \cdots, x_M, y_1, \cdots, y_N\}$ to represent the state of the network, *i.e.* the state x of each of its M edges and the state y of each of its N nodes, where $x_i = 1$ if edge e_i is operating and 0 otherwise (y for node). For simplicity of illustration, we assume that nodes cannot fail, while edges can (thus y is no longer considered hereafter). The state of the network is defined as being *non-failure* if the specified terminal-pair is connected by at least one path of operating edges; otherwise it is *failure*. All possible *failure* states are included in the subset Ω_F of the set Ω containing all possible scenarios (*failure* and *non-failure*). An inclusive TPR analysis requires considering all elements in Ω_F. We then define the TPR as:

$$R_{sd} = \Pr\left(\phi_{sd}\left(S_k\right) = 1\right), S_k \in \Omega \tag{3}$$

where ϕ_{sd} is a binary function which indicates the connection availability between node-pair s and d (1 = connection; 0 = no-connection). Let us assume that each edge e_i has associated a probability p_i of being operating and a probability $q_i = 1 - p_i$ of being failed; then, the TPR of the network can be calculated as:

$$R_{sd} = 1 - \sum_{S_k \in \Omega_F} \left(\prod_{x_i \notin X_f} \left(1 - p_i\right) \prod_{x_i \in X_f} p_i \right) \tag{4}$$

where x_i represents the state of network edge e_i and X_f is the set of failed edges for a given state $S_k \in \Omega_F$. Note that the implicit assumption underpinning Equation (4) is that the network edges are independent.

When the computational cost of the network is high (it grows exponentially with the number of network components), then, the artificial network at a suitable level of the hierarchy can be leveraged to carry out the TPR. At the generic level of the hierarchy, the artificial link $E_{ij}^{(l)}$ connecting nodes (clusters) $V_i^{(l)}$ and $V_j^{(l)}$ is composed by actual network links in parallel,

$$E_{ij}^{(l)} = \left\{ e_{st} \middle| v_s \in V_i^{(l)}, v_t \in V_j^{(l)} \right\};$$

then, the reliability of the artificial edge $E_{ij}^{(l)}$ at level l can be calculated by:

$$p\left(E_{ij}^{(l)}\right) = 1 - \prod_{e_{st} \in E_{ij}^{(l)}} q\left(e_{st}\right);\ v_s \in V_i^{(l)}, v_t \in V_j^{(l)} \tag{5}$$

where $q\left(e_{st}\right)$ indicates the failure probability of the actual link e_{st} that in the real network connects nodes v_s and v_t.

Various algorithms to solve the classic TPR problem have been reported in literature, with various computational efficiencies [29-31]. A so-called Modified Dotson algorithm [30], which has been claimed and tested to subdue others in computational time, is used here for the TPR assessment based on the hierarchical modeling. The failure probability of the transmission lines in the IPTN system is computed based on outage statistics provided in [32], by assuming that the edge failure probability is proportional to its length with an average failure rate $\lambda = 1.380635$ occ/100mile-year, and average outage duration time t = 64.81 hours/occ.

In **Figure 3** right-panel, the connection reliability between nodes 1 and 127 in the IPTN network system (left panel in **Figure 3**) is shown as resulting from evaluations at each of the five levels of the hierarchical model described in the previous Section. The right panel of **Figure 3** gives the probabilities of connectivity failure between nodes 1 and 127 from level 2 to level 5 (top) and

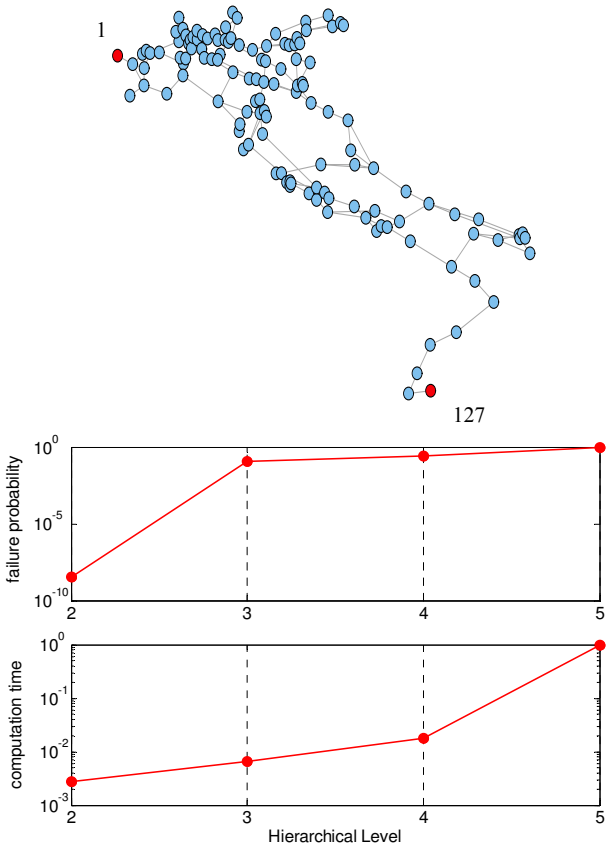


Figure 3. Illustrative example of terminal pair reliability assessment of IPTN system.

the computational time needed for the analysis (bottom); the values have been normalized with respect to the maximum values of connectivity failure probability and computational time, which occur at the bottom of the hierarchy (level 5) corresponding to the whole network. The result at the first level has not been shown since its value is simply 0, *i.e.*, node 1 and 127 are in a single unit and will not disconnect. One can see that the difference between the actual and estimated failure probabilities decreases as the assessment moves downs to the bottom of the hierarchy, balanced by the computation time which instead increases significantly. The decision maker can obtain satisfying estimations of the failure probability at a hierarchical level of lower complexity, e.g. level 3, thus saving significantly in computation time.

3.2. Component Extended Importance Measures

Component importance measures are widely used in system engineering to identify components within the system that most significantly influence the system behavior with respect to reliability, risk and/or safety. The indications drawn are valuable for establishing direction and prioritization of actions, related to reliability improvement during system design and optimization of operation and maintenance.

A well known IM is the so called Birnbaum IM defined as (with reference to system reliability R_s, as the system performance indicator) [14]:

$$I_i^B = \frac{\partial R_s}{\partial R_i} = R_s\left(R_i = 1\right) - R_s\left(R_i = 0\right) \tag{6}$$

where I_i^B is the Birnbaum Importance (BI) of component *i*; R_s represents the reliability of the system; R_i is the reliability of component *i*; $R_s\left(R_i = 1\right)$ is the system reliability calculated assuming that component *i* is perfectly operating and $R_s\left(R_i = 0\right)$ the system reliability in the opposite case of component *i* failed. The BI measures the significance of component *i* to system reliability by the rate at which system reliability improves with the reliability of component *i*. As shown in Equation (6), the BI of component *i* does not depend on R_i itself, so that two components *i* and *j* may have a similar value I^B although they have different reliability values R_i and R_j, respectively; this could be seen as a limitation of BI.

The Criticality Importance (CI) measure overcomes the above limitation by considering component unreliability [17]. It is defined as:

$$I_i^C = I_i^{BI}\frac{F_i}{F_s} = \left[R_s\left(R_i = 1\right) - R_s\left(R_i = 0\right)\right]\frac{1-R_i}{F_s} \tag{7}$$

where F_i is the unreliability of component *i* and F_s is the system unreliability. Now, a less reliable component is more critical than another one with same value of BI.

Fuessell & Vesely [15] proposed an alternative importance measure according to which the importance of a component in the system depends on the number and on the order of the cut sets in which it appears [17]. Most commonly used as a risk reduction indicator, Fuessell & Vesely Importance (FVI) quantifies the maximum decrement in system reliability caused by a particular component being failed $\left(R_i = 0\right)$:

$$I_i^{FV} = \frac{R_s - R_s\left(R_i = 0\right)}{R_s} \tag{8}$$

The previously proposed *IMs* (*BI*, *CI* and *FVI*) are functionally different. They evaluate subtly different properties of the system behavior, and therefore, are often used in a complementary fashion to infer different information. To apply the IMs for analyzing a network system such as the IPTN, it is necessary to extend the definition of the IMs to account for the multiple terminal or node pairs (e.g. generator-distributor pairs) where connectivity defines the network functionality.

Specializing such extension for the analysis of the importance of components of the IPTN system, we introduce the Extended Birnbaum Importance (EBI) measure as the average of all BI values obtained considering all possible Generator-Distributor pairs reliabilities in the network system:

$$\begin{aligned} I_i^{E-B} &= \frac{1}{N_G N_D}\sum_{s\in V_G, d\in V_D}\frac{\partial R_{sd}}{\partial R_i} \\ &= \frac{1}{N_G N_D}\sum_{s\in V_G, d\in V_D}\left(R_{sd}\left(R_i = 1\right) - R_{sd}\left(R_i = 0\right)\right) \end{aligned} \tag{9}$$

where N_G and N_D are the number of generators and distributors in the network respectively; V_G and V_D are sets of node generators and distributors respectively; R_{sd} is the TPR between node *s* and node *d*; $R_{sd}\left(R_i = 1\right)$ and $R_{sd}\left(R_i = 0\right)$ represent the terminal pair reliabilities between node *s* and node *d*, in the condition that component *i* is perfectly operating and completely failed, respectively.

Similarly, we can define Extended Criticality Importance (ECI) and Extended Fussell &Vesely Importance (EFVI) measures:

$$I_i^{E-C} = \frac{1}{N_G N_D}\sum_{s\in V_G, d\in V_D}\left[R_{sd}\left(R_i = 1\right) - R_{sd}\left(R_i = 0\right)\right]\frac{1-R_i}{1-R_{sd}} \tag{10}$$

$$I_i^{E-FV} = \frac{1}{N_G N_D}\sum_{s\in V_G, d\in V_D}\frac{R_{sd} - R_{sd}\left(R_i = 0\right)}{R_{sd}} \tag{11}$$

where I_i^{E-C} is the Extended Criticality Importance (ECI) measure of component *i* and I_i^{E-FV} is the Extended Fussell & Vesely Importance measure.

3.3. Numerical Example: Results and Discussions

The EIMs introduced have been calculated for the IPTN system at different levels of the hierarchical model of the system developed. For the evaluation, an artificial node functions as a generator as long as there is at least one actual generator node within it; otherwise it is simply a distributor.

Tables 2 and **3** report the results of the importance assessment (EBI, EFVI are given in **Table 2** and ECI in **Table 3**) for the artificial edges of the network at level 2 of the hierarchy. For EBI and EFVI, all components in the artificial network have the same importance rank, but with slight differences between EBI and EFVI values, and the artificial edge {2-4} is the most important in the artificial network (see the bottom panel of **Figure 2**). This is due to the fact that this artificial edge is the only possible link between a generator in artificial node $V_2^{(2)}$ and the distributors in other artificial nodes, and thus its disconnection would cause a large-scale generator-distributor connectivity failure. The rank based on the ECI is different from that of EBI and EFVI, and the most important artificial edge is {3-4}; the difference lies in the definition, as discussed before: EBI depends only on the structure of the system and not on the reliability of the considered component, whereas ECI takes the unreliability of the component into consideration, and in fact, the artificial edge {3-4} is made of only one actual edge with relatively high probability of failure, which leads to the highest ECI value.

By combining the indications of EBI and ECI, it is advisable to offer advices to the decision maker for the purpose of system maintenance and operation optimization [10]. When EBI & EFVI is high and ECI is low like in the case of artificial edge {2-4}, the system safety can be improved by protecting against failure of each component, e.g., adding alternative edges between artificial node $V_2^{(2)}$ and node $V_1^{(2)}$ (or $V_3^{(2)}$). For the case of low EBI & EFVI and high ECI (artificial edge {3-4}), the decision maker should invest in improvements of the component itself, to decrease the failure probability.

Tables 4 and **5** report the evaluation results at level 3 of the hierarchy. Fictitious edge {4-9}, composed by actual edges {110-111, 112-114, 107-109}, has highest EBI and EFVI values but relatively low ECI value (ranked 15th among all 17 artificial edges), indicating that the system reliability is highly sensitive to its failure, whereas the component itself is relatively reliable. On the contrary, the artificial edge {1-10} composed by only one actual edge {64-78} is highly unreliable itself, and its EBI and EFVI values are both ranked 8th among all 17 edges. It is important to pay attention to these artificial edges with both relatively high EBI & EFVI ranks and ECI ranks, which means not only that their failures cause a significant deterioration of the system reliability but also that they are vulnerable themselves. In this respect, by combining **Tables 4** and **5**, we find that artificial edges {1-11} (whose actual network link is {71-83}), {6-10} (which is composed by actual link {76-79}), and {10-12} (which is composed by actual links {75-88, 80-95}) are the three artificial edges most critical for the system reliability.

The bold edges in **Figure 4** represent the edges of the actual network system which have resulted most critical based on the extended importance measure evaluation carried out at level 3 of the hierarchy model. These edges should be paid special attention. For links {110-111, 112-114, 107-109}, improving the defense in depth against

Table 2. EBI and EFVI at level 2 of the hierarchical model.

Artificial Edge	EBI		EFVI		Associated Actual Edges
	Rank	Value	Rank	Value	
{2-4}	1	0.3750	1	0.3750	{107-109,112-114,110-111}
{1-4}	2	1.9606E − 03	2	1.9605E − 03	{64-78,71-83}
{1-3}	3	1.4817E − 03	3	1.4817E − 03	{59-60,61-62,30-34,30-31}
{3-4}	4	1.5100E − 05	4	1.4900E − 05	{76-79}

Table 3. ECI at level 2 of the hierarchical model.

Artificial Edges	Rank	ECI	Associated Actual Edges
{2-4}	4	0.37	{107-109,112-114,110-111}
{1-4}	2	7699812.62	{64-78,71-83}
{1-3}	3	16.55	{59-60,61-62,30-34,30-31}
{3-4}	1	7699828.67	{76-79}

Table 4. EBI and EFVI at level 3 of the hierarchical model.

Artificial Edges	EBI		EFVI		Associated Actual Edges
	Rank	Value	Rank	Value	
{4-9}	1	0.2867	1	0.2879	{110-111, 112-114, 107-109}
{4-5}	2	0.1591	2	0.1591	{119-122}
{9-12}	3	0.0030	3	0.0030	{98-99, 94-97, 97-98}
{10-12}	4	0.0028	4	0.0028	{75-88, 80-95}
{2-3}	5	0.0007	5	0.0007	{42-43, 40-43}
{1-11}	6	0.0002	6	0.0002	{71-83}
{6-10}	7	1.55E − 05	7	1.54E − 05	{76-79}
{1-10}	8	1.17E − 05	8	1.15E − 05	{64-78}
{3-8}	9	8.04E − 06	9	8.05E − 06	{30-31, 30-34, 59-60}
{9-11}	10	7.52E − 06	10	7.38E − 06	{102-110}
{11-12}	11	4.82E − 06	11	4.65E − 06	{86-88}
{7-8}	12	4.11E − 06	12	4.11E − 06	{10-16, 10-21, 20-21}
{1-2}	13	3.00E − 06	13	2.98E − 06	{47-48}
{1-3}	14	8.43E − 08	14	8.40E − 08	{40-41, 60-63}
{1-6}	15	7.58E − 08	16	5.56E − 08	{61-62}
{6-7}	16	5.58E − 08	15	4.96E − 08	{11-12, 12-13}
{6-8}	17	1.43E − 08	17	3.92E − 08	{59-61}

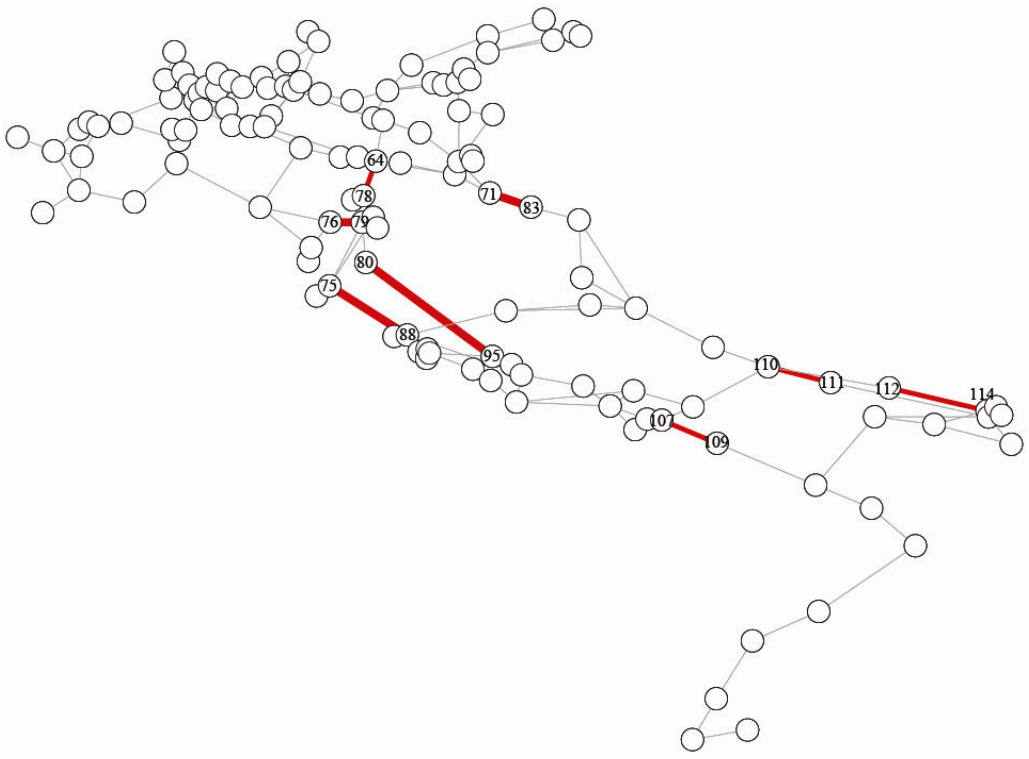


Figure 4. Most critical edges at level 3 of the hierarchical model.

Table 5. The results of ECI assessment at level 3 of the hierarchical model.

Artificial Edges	Rank	ECI	Associated Actual Edges
{1-10}	1	3029896	{64-78}
{6-10}	2	2975998	{76-79}
{1-11}	3	2763614	{71-83}
{10-12}	4	139883.50	{75-88, 80-95}
{11-12}	5	45071.41	{86-88}
{6-8}	6	24763.84	{59-61}
{1-6}	7	20374.07	{61-62}
{1-2}	8	13626.99	{47-48}
{1-3}	9	212.10	{40-41, 60-63}
{6-7}	10	196.24	{11-12, 12-13}
{2-3}	11	57.85	{42-43, 40-43}
{3-8}	12	10.65	{30-31, 30-34, 59-60}
{7-8}	13	0.38	{10-16, 10-21, 20-21}
{4-5}	14	0.16	{119-122}
{4-9}	15	0.07	{110-111, 112-114, 107-109}
{9-11}	16	0.05	{102-110}
{9-12}	17	0.02	{98-99, 94-97, 97-98}

their failures is advisable to improve the reliability of the system, while for links {64-78, 71-83, 76-79, 80-95, 75-88}, the edge unreliability should also be mitigated.

Tables 6 and **7** report the results of the EIMs evaluation at level 4 of the IPTN hierarchical model. It turns out that artificial edge {7-11} (corresponding to actual link {119-122}) has the highest EBI and EFVI values and artificial edge {1-22} (corresponding to actual link {64-78}) has the highest ECI rank and relatively high EBI and EFVI ranks, indicating its criticality to system reliability.

Finally, **Table 8** reports the computation times required for the calculations of the EIMs at different levels in the hierarchy: as expected, the more we go down in the hierarchy the higher the computation time.

4. Conclusions

The modeling and analysis of complex network systems is a non-trivial task. Related decision-making regarding reliability and vulnerability is limited by computational resources.

In this work, we have introduced a framework for hierarchical modeling of complex network systems, which leads to the definition of different varied-size grained artificial networks. The construction of the hierarchical model is obtained by a recursive unsupervised spectral clustering method. The hierarchical model thereby obtained provides a multi-scaled representation of the original network system, with more detailed information but high complexity at the lower levels of the hierarchy, and simplified structure but relatively low complexity at the higher levels. The availability of different scales of modeling resolution allows a flexible management of the analysis, at the level of details desired for its purposes. The 380 kV Italian Power Transmission Network (IPTN) has been taken as an illustration.

Furthermore, Importance Measures (IMs) such as Birnbaum, Fuessell & Vesely and Criticality, have been extended for application to the terminal-pair reliability problem in complex distributed network systems.

The calculation of the extended IMs at different levels of the hierarchical system modeling has demonstrated the effectiveness of the proposed hierarchical modeling, with the IM-ranking of the IPTN elements offering insights on how to improve the system against failures of most critical elements.

5. Acknowledgements

The authors are thankful to Dr. Giovanni Sansavini of Politecnico di Milano for supporting the work with rele-

Table 6. EBI and EFVI at level 4 of the hierarchical model (Only the top 20 elements are reported).

Artificial Edges	EBI		EFVI		Associated Actual Edges
	Rank	Value	Rank	Value	
{7-11}	1	0.1504	1	0.1511	{119-122}
{3-4}	2	0.0787	2	0.0788	{47-49,51-54}
{10-11}	3	0.0782	3	0.0788	{125-126}
{22-23}	4	4.2717E − 4	4	4.2606E − 4	{78-81}
{24-25}	5	3.5490E − 4	5	3.5551E − 4	{84-101,85-101}
{12-13}	6	3.3570E − 4	6	3.3605E − 4	{14-73,14-76}
{1-22}	7	3.0044E − 4	7	2.9915E − 4	{64-78}
{21-28}	8	2.1515E − 4	8	2.1436E − 4	{94-97}
{26-28}	9	1.7038E − 4	9	1.6954E − 4	{92-93}
{2-25}	10	1.6962E − 4	10	1.6906E − 4	{71-83}
{17-19}	11	1.0216E − 4	11	1.0206E − 4	{17-18}
{14-19}	12	7.53E − 05	12	7.51E − 05	{10-16}
{23-29}	13	6.50E − 05	13	6.43E − 05	{75-88}
{7-21}	14	5.10E − 05	14	5.09E − 05	{107-109}
{9-20}	15	4.24E − 05	16	4.22E − 05	{110-111}
{23-27}	16	3.74E − 05	15	3.66E − 05	{80-95}
{13-23}	17	3.36E − 05	17	3.35E − 05	{76-79}
{21-27}	18	3.22E − 05	18	3.23E − 05	{97-98,98-99}
{7-8}	19	3.07E − 05	19	3.07E − 05	{113-120}
{8-20}	20	2.64E − 05	20	2.61E − 05	{112-114}

Table 7. ECI at level 4 of the hierarchical model (Only the top 20 elements are reported).

Artificial Edges	Rank	ECI	Associated Actual Edges
{1-22}	1	868094.790	{64-78}
{2-4}	2	750781.848	{47-48}
{1-12}	3	737490.646	{61-62}
{13-23}	4	645088.015	{76-79}
{22-23}	5	602356.820	{78-81}
{12-14}	6	44554.9988	{12-13}
{14-18}	7	43748.7434	{10-21}
{14-15}	8	40914.4150	{7-9}
{14-19}	9	23137.9590	{10-16}
{17-19}	10	17031.1229	{17-18}
{12-13}	11	14138.4808	{14-73,14-76}
{12-18}	12	8829.8833	{59-61}
{1-5}	13	6285.1115	{40-41,60-63}
{5-16}	14	6013.8315	{30-31}
{16-18}	15	5235.8073	{27-59}
{6-16}	16	5051.5230	{30-34}
{5-18}	17	4665.6252	{59-60}
{15-18}	18	2481.7982	{20-21}
{12-15}	19	1666.1408	{11-12}
{4-5}	20	325.9829	{40-43}

Table 8. EIMs evaluation time at each level of the hierarchical model.

EIMs	Computation time (seconds on a computer with 2 CPU 3.06 G 3.07 G)		
	Level 2	Level 3	Level 4
EBI	0.3856	108.5	31763.58
EFVI	0.2086	112.2	32179.50
ECI	0.5152	175.0	47621.58

vant information on the network structure used as reference system and to Dr. Yanfu Li of Supelec for fruitful discussions.

REFERENCES

[1] W. Kröger, "Critical Infrastructures at Risk: A Need for a New Conceptual Approach and Extended Analytical Tools," *Reliability Engineering & System Safety*, Vol. 93, No. 12, 2008, pp. 1781-1787. doi:10.1016/j.ress.2008.03.005

[2] E. Zio, "Reliability Engineering: Old Problems and New Challenges," *Reliability Engineering & System Safety*, Vol. 94, No. 2, 2009, pp. 125-141. doi:10.1016/j.ress.2008.06.002

[3] W. Kröger and E. Zio, "Vulnerable Systems," Springer, Berlin, 2011. doi:10.1007/978-0-85729-655-9

[4] A. Mason, J. Onnela and P. Mucha, "Communities in Networks," *Notices of the American Mathematical Society*, Vol. 56, No. 9, 2009, pp. 1082-1166.

[5] S. Fortunato, "Community Detection in Graphs," *Physics Reports*, Vol. 486, No. 3, 2010, pp. 75-174. doi:10.1016/j.physrep.2009.11.002

[6] B. Karrer, E. Levina and M. Newman, "Robustness of Community Structure in Networks," *Physical Review E*, Vol. 77, No. 4, 2008, Article ID: 046119. doi:10.1103/PhysRevE.77.046119

[7] A. Clauset, C. Moore and M. E. J. Newman, "Hierarchical Structure and the Prediction of Missing Links in Networks," *Nature*, Vol. 453, No. 7191, 2008, pp. 98-101. doi:10.1038/nature06830

[8] M. Sales-Pardo, R. Guimerá, A. Moreira, A. Moreira and L. A. N. Amaral, "Extracting the Hierarchical Organization of Complex Systems," *Proceedings of the National Academy of Sciences*, Vol. 104, No. 39, 2007, pp. 15224-15229. doi:10.1073/pnas.0703740104

[9] C. Gómez, M. Sánchez-Silva and L.Duenas-Osorio, "Clustering Methods for Risk Assessment of Infrastructure Network Systems," In: Faber, Köhler and Nishijima, Eds., *Applications of Statistics and Probability in Civil Engineering*, CRC Press, Boca Raton, 2011.

[10] M. Van der Borst and H. Schoonakker, "An Overview of PSA Importance Measures," *Reliability Engineering & System Safety*, Vol. 72, No. 3, 2001, pp. 241-245. doi:10.1016/S0951-8320(01)00007-2

[11] I. Gertsbakh and Y. Shpungin, "Network Reliability Importance Measures: Combinatorics and Monte Carlo Based Computations," *WSEAS Transactions on Computers*, Vol. 7, No. 4, 2008, pp. 216-227.

[12] E. Zio, "Computational Methods for Reliability and Risk Analysis," World Scientific Publishing, Singapore, 2009. doi:10.1142/7190

[13] E. Zio, "Risk Importance Measures," In: *Safety and Risk Modeling and its Applications*, Springer, Berlin, 2011.

[14] Z. W. Birnbaum, "On the Importance of Different Components in a Multicomponent System," In: P. R. Krishnaiah, Ed., *Multivariate Analysis II*, Academic Press, New York, 1969.

[15] J. B. Fussell, "How to Hand-Calculate System Reliability and Safety Characteristics," *IEEE Transactions on Reliability*, Vol. 24, No. 3, 1975, pp. 169-174. doi:10.1109/TR.1975.5215142

[16] M. C. Cheok, W. P. Gareth and R. Sherry, "Use of Importance Measures in Risk-informed Regulatory Applications," *Reliability Engineering & System Safety*, Vol. 60, No. 3, 1998, pp. 213-226. doi:10.1016/S0951-8320(97)00144-0

[17] J. F. Espiritu, D. W. Coit and U. Prakash, "Component Criticality Importance Measures for the Power Industry," *Electric Power Systems Research*, Vol. 77, No. 5, 2007, pp. 407-420. doi:10.1016/j.epsr.2006.04.003

[18] V. Latora and M. Marchiori, "Economic Small-World Behavior in Weighted Networks," *The European Physical Journal B—Condensed Matter and Complex Systems*, Vol. 32, No. 2, 2003, pp. 249-263. doi:10.1140/epjb/e2003-00095-5

[19] U. Brandes and T. Erlebach, "Network Analysis: Methodological Foundations," Springer, Berlin, 2005.

[20] E. Zio and G. Sansavini, "Component Criticality in Failure Cascade Processes of Network Systems," *Risk Analysis*, Vol. 31, No. 8, 2011, pp. 1196-1210. doi:10.1111/j.1539-6924.2011.01584.x

[21] V. Rosato, S. Bologna and F. Tiriticco "Topological Properties of High-Voltage Electrical Transmission Networks," *Electric Power Systems Research*, Vol. 77, No. 2, 2007, pp. 99-105. doi:10.1016/j.epsr.2005.05.013

[22] E. Ravasz and B. Albert-László, "Hierarchical Organization in Complex Networks," *Physical Review E*, Vol. 67, No. 2, 2003, Article ID: 026112. doi:10.1103/PhysRevE.67.026112

[23] Von Luxburg and Ulrike, "A Tutorial on Spectral Clustering," *Statistics and Computing*, Vol. 17, No. 4, 2007, pp. 395-416. doi:10.1007/s11222-007-9033-z

[24] A. K. Jain, M. Narasimha Murty and P. J. Flynn, "Data Clustering: A Review," *ACM Computing Surveys*, Vol. 31, No. 3, 1999, pp. 264-323.

[25] M. Filippone, F. Camastra, F. Masulli and S. Rovetta, "A Survey of Kernel and Spectral Methods for Clustering," *Pattern Recognition*, Vol. 41, No. 1, 2008, pp. 176-190. doi:10.1016/j.patcog.2007.05.018

[26] S. E. Schaeffer, "Graph Clustering," *Computer Science Review*, Vol. 1, No. 1, 2007, pp. 27-64. doi:10.1016/j.cosrev.2007.05.001

[27] S. Leguizemón, H. Pelgrum and S. Azzali, "Unsupervised Fuzzy C-means Classification for the Determination of Dynamically Homogeneous Areas," *Revista SELPER*, Vol. 12, No. 12, 1996, pp. 20-24.

[28] M. Alata, M. Molhim and A. Ramini, "Optimizing of Fuzzy C-Means Clustering Algorithm Using GA," *World Academy of Science*, *Engineering and Technology*, Vol. 1, No. 5, 2008, pp. 224-229.

[29] W. Dotson and J. Gobien, "A New Analysis Technique for Probabilistic Graphs," *IEEE Transactions on Circuits and Systems*, Vol. 26, No. 10, 1979, pp. 855-865. doi:10.1109/TCS.1979.1084573

[30] Y. B. Yoo and N. Deo., "A Comparison of Algorithms for Terminal-pair Reliability," *IEEE Transactions on Reliability*, Vol. 37, No. 2, 1988, pp. 210-215.

[31] C.-C. Jane, W.-H. Shen and Y.-W. Laih, "Practical Sequential Bounds for Approximating Two-Terminal Reliability," *European Journal of Operational Research*, Vol. 195, No. 2, 2009, pp. 427-441. doi:10.1016/j.ejor.2008.02.022

[32] A. A. Chowdhury and D. O. Koval, "High Voltage Transmission Equipment Forced Outage Statistics Including Different Fault Types," *Proceedings of the* 10*th International Conference on Probabilistic Methods Applied to Power Systems*, 25-29 May 2008, pp.1-8, 25-29.

Paper [3] Y.-P. Fang, N. Pedroni, E. Zio. "Network-centric Optimization of Failure Resilient Electrical Infrastructures and its Validation by Power Flow Model." Risk Analysis, Accepted, 2014.

Optimization of Cascade-Resilient Electrical Infrastructures and its Validation by Power Flow Modelling

Yiping Fang[1], Nicola Pedroni[1], Enrico Zio[1,2]

[1]*Chair on Systems Science and the Energetic challenge*
Ecole Centrale Paris and Supelec, France

[2]*Energy Department, Politecnico di Milano, Italy*

ABSTRACT

Large scale outages on real-world critical infrastructures (CIs), although infrequent, are increasingly disastrous to our society. In this paper, we are primarily concerned with power transmission networks and we consider the problem of allocation of generation to distributors by rewiring links under the objectives of maximizing network resilience to cascading failure and minimizing investment costs. The combinatorial multi-objective optimization is carried out by a non-dominated sorting binary differential evolution (NSBDE) algorithm. For each generators-distributors connection pattern considered in the NSBDE search, a computationally-cheap, topological model of failure cascading in a complex network (named, the Motter-Lai (ML) model) is used to simulate and quantify network resilience to cascading failures initiated by targeted attacks. The results on the 400kV French power transmission network case study show that the proposed method allows to identify optimal patterns of generators-distributors connection which improve cascading resilience at an acceptable cost.

To verify the realistic character of the results obtained by the NSBDE with embedded ML topological model, a more realistic but also more computationally-expensive model of cascading failures is adopted, based on optimal power flow (namely, the ORNL-Pserc-Alaska (OPA) model). The consistent results between the two models provide impetus for the use of topological, complex network theory models for analysis and optimization of large infrastructures against cascading failure with the advantages of simplicity, scalability and low computational cost.

KEY WORDS: critical infrastructure, power transmission network, cascading failures, complex network theory model, power flow model, optimization

1 INTRODUCTION

Our modern society has come to depend on large-scale critical infrastructures (CIs) to deliver resources and services to consumers and businesses in an efficient manner. These CIs are complex networks of interconnected functional and structural elements. Large scale outages on these real-world complex networks, although infrequent, are increasingly disastrous to society, with estimates of direct

costs up to billions of dollars and inestimable indirect costs. Typical examples include blackouts in power transmission networks [1-3], financial bankruptcy [4], telecommunication outages [5], and catastrophic failures in socio-economic systems [6-7].

Cascading failures are initiated typically when a small part of the system fails for some reasons, and the load on that part (i.e. the flow passing through it) must be redistributed to other parts in the system. This redistribution may cause other components to exceed their capacity causing them also to fail. Hence, the number of failed or stressed components increases, propagating throughout the network. In particularly serious cases, the entire network is affected. Research regarding modeling, prediction and mitigation of cascading failures in CIs, whereby small initial disturbances may propagate through the whole infrastructure system, has addressed the problem in different ways [4-6, 8-13].

Albert et al. [14] demonstrated that the vulnerability of modern infrastructure networks (e.g., power transmission networks) is inherent to their structure. Thadakamalla [15] revealed that the topology of a supply infrastructure has great impact on its resilience. Then, much attention has been paid in recent years in the direction of network topology optimization, with the purpose of achieving desired targets of reliability and/or resilience [16-19, 26]. Shao et al. [17] proposed a shrinking and searching algorithm to maximize the reliability of a distributed access network with constrained total cost; however, the intense computational cost for evaluating network reliability prohibits the application of the model to large size networks. Gutfraind [18] introduced a multi-objective optimization method for constructing cascade resilient networks based on the structure of terrorist networks. Besides, Newth et al. [19] used a modified Metropolis evolutionary algorithm to evolve failure resilient networks with the objective of maximizing the average network efficiency. Cadini et al. [20] investigated the problem of optimizing the transmission reliability efficiency of an existing power transmission network with least cost by adding new connection links.

In practical cases, the cost of knocking down an existing network and reconstructing it from scratch is prohibitive, especially for CIs like the power transmission network. A more practicable alternative is to reconfigure parts of the network topology, e.g. by reallocation of the links which connect production facilities to consumers.

The primary objective of this paper is to propose a methodology for optimal allocation of the links connecting generators and distributors in a power transmission network for obtaining high resilience to cascading failures while keeping the investment costs low. Formulated as a large-scale, nonlinear and combinatorial multi-objective optimization problem, the facility allocation problem is solved by an evolutionary method, i.e., the non-dominated sorting binary differential evolution (NSBDE) algorithm [21, 22].

The search by the NSBDE requires also: (i) the construction of a model to describe the cascading failure process in the network of interest, and (ii) the repeated evaluation of the model for every possible generators-distributors configuration proposed by the algorithm during the search. With respect to the model, two approaches are typically considered in the analysis of power transmission systems: *complex network theory* models, such as the Motter-Lai (ML) model [8, 9] and *artificial power flow models*, such as the ORNL-Pserc-Alaska (OPA) model [10-12]. These approaches provide different tradeoffs between the (relatively low) computational cost associated to the model evaluation (allowing real-time applications to large scale power grids) and the (high) level of detail in the system description (including physical characteristics and power flows constraints), respectively.

The OPA model seeks to faithfully describe the dispatching dynamics of the power flows during the evolution of the failure propagation following the initial disturbances, by explicitly incorporating the standard DC power flow equations and minimizing generation cost and load shedding [11]. Embracing this more physical description and solving the constrained linear optimization functions associated to the model, result in a significant increase in the computational burden, rendering its application extremely difficult for realistic networks with large number of elements [13].

For these reasons, topological models based on complex network theory (e.g. the ML model) have emerged in recent years [8, 9, 23-25]. In particular, the ML model is a relatively simple and abstract model relying on the resemblance of complex networks to electrical infrastructure systems (in terms of graph theory). It has the advantage of modelling cascading dynamics with few parameters, so that its application to realistic, large-scale networks is feasible and certainly more readily than OPA [23]. However, ML abstracts the power flow laws and constraints of the electrical system. Inevitably, then, it cannot provide direct physical measures of blackout size, but rather abstract measures such as efficiency loss. This has posed questions on whether or not it is adequate in practice, due to its abstract nature, although it has been recognized to offer a new and interesting perspective on the study of cascading failures on power grids [24].

It is worth mentioning that studies tackling the problem of validation of network-centric approaches are few in literature. Some studies [13, 24] have provided qualitative comparisons between complex network theory models and power flow models – identifying similarities and differences, and evaluating advantages and disadvantages. Most recently, Correa and Yusta [26] conclude on the appropriateness of graph theory techniques for the assessment of electric network vulnerability by means of comparisons between physical power flow models and scale-free graph statistic indexes. Cupac et al. [27] have presented a method to quantitatively compare a network-centric model (CLM) and the power flow model OPA, finding that the CLM model exhibits overall properties which are consistent with the more realistic OPA fast-scale model. On the other hand, Fitzmaurice et al. [40] find that the topological nearest neighbor cascading failure model (namely, the TC model) shows different

characteristics from two other Kirchhoff models, namely LD and QSS. Hines et al. [41] conclude that evaluating vulnerability in power networks using purely topological metrics may be misleading under some circumstances. Furthermore, Cotilla-Sanchez et al. [42] propose a new method for representing electrical structures using electrical distances rather than geographic connections.

In the present paper, we embrace the topological ML cascading failure model and embed it in the NSBDE for optimally solving the problem of generators-distributors link allocation. For exemplification, we apply the method to the 400 kV French power transmission network, under the objectives of maximizing network resilience to cascading failures and minimizing investment costs [28]. We, then, tackle the problem of realistic significance of the results that can be obtained with the proposed methodology. For this reason, the OPA is performed on the optimal network topologies found. To the authors' knowledge, this is the first study addressing the validation of optimization based on a topological cascade model (namely, the ML model), by applying a more realistic power flow model (namely, the OPA model).

The optimization problem considered is addressing the network topology and in the specific case study we have considered for exemplification purpose the topology abstracted from the 400kV French power grid. In the abstraction, any station (generator, transmission/distribution substation) is regarded as one individual topological node in the network model, whereas the internal structure and functional logic of the specific station are ignored. Then, how the transmission lines interconnect with lower voltage networks has not been considered in this study, similar to what has been done in prior studies on these analyses [18-20]. The purpose of performing these analyses in this way is to leverage the simplicity and low computational cost of the topological (cascading failure) model used within the (evolutionary) network optimization, which otherwise would be very costly.

The remainder of this paper is organized as follows. In Section 2, we introduce the ML and OPA cascading failure models in detail. We, then, formulate the multi-objective optimization problem taking investment costs and failure resilience into account in Section 3. Section 4 unveils the detailed procedure of the proposed NSBDE algorithm. Section 5 illustrates the French 400kV power transmission network case study and the analysis and evaluation of the results. Discussion and conclusion are drawn in Section 6.

2 CASCADING FAILURE MODELS CONSIDERED IN THIS WORK

Modelling the dynamic evolution of system-wide cascading failure processes poses a number of challenges due to the diversity of mechanisms which can initiate the initial failure and influence the subsequent propagation of breakdowns in the power system [13]. Various cascading failure models have been proposed; these can be divided into two main categories: those based on complex network theory

analysis and those using power flow analysis, often including optimal economic power dispatch after each failure in the propagation, e.g., by linear optimal power flow (OPF) [27].

Complex network theory models, including the ML model adopted in this work as described in Section 2.1 below, abstract the representation of a power grid as a graph and, then, study the connectivity characteristics, the propagation mechanisms through the graph connections and their relationships. They typically consider flows of discrete packets that are injected and removed from all nodes and follow least-distance paths, and the importance of links or nodes is measured by their "betweenness", which is proportional to the number of least-distance paths through the link or node [13]. Among these, the ML model is the most widely used and a relatively simple one. These types of models have proved to provide a good understanding of the specific grid dynamics of cascading failures [30]. However, in these models the assumptions only abstract the real loading of the components and the flow distribution through the connections. For this reason, it is necessary to ascertain the meaningfulness of the results for real electrical infrastructures.

Power flow models, on the contrary, are based on realistic power flow equations to describe the flow dispatching dynamics and failure evolution after the initial disturbances in the power grid. The OPA model, which is the most commonly used among these types of models, is introduced in Section 2.2 below; it is based on the linearized or DC power flow approximation, which has been proved to be able to give a good approximation of active power flows in the network [29]. Another power flow model is the CASCADE model [43], though it is considered ''too simple'' in that it ''disregards the system structure, neglects the times between adjacent failures and generation adaptation during failure'' [44].

2.1. The ML model

The ML model has been proposed by Motter and Lai [8], with extensions to differentiate generators and loads [23]. The power transmission network is represented as an undirected graph Q with a set of N nodes representing N_G generators and N_D loads representing distribution substations, interconnected by a set of edges representing transmission lines. The structure of the network is identified by an $N \times N$ interaction matrix W, whose element w_{ij} is 0 if node i and j are not connected directly; otherwise it is assigned 1 for an unweighted network or a numerical value between i and j for a weighted network.

The ML model assumes that at each time step, one unit of the relevant quantity (electrical flow for power grids) is exchanged between every pair of generator and distributor nodes, and transmitted along the shortest path connecting them. The flow at one node is, then, the number of shortest paths passing through it. More precisely, the flow L_k passing through node k is quantified by the node betweenness calculated as the fraction of the generator-distributor shortest paths passing through that node:

$$L_k = \frac{1}{N_G N_D} \sum_{i \in V_G, j \in V_D, i \neq j \neq k} \frac{n_{ij}(k)}{n_{ij}} \quad (1)$$

where n_{ij} is the number of shortest paths between generator nodes and distributor nodes, and $n_{ij}(k)$ is the number of generator-distributor shortest paths passing though node *k*.

The capacity of node *k* is assumed to be proportional to its initial node L_k with a network tolerance parameter α,

$$C_k = (1 + \alpha) L_k \quad (2)$$

The concept of the tolerance parameter α ($\alpha > 0$) can be understood as an operating margin allowing safe operation of the component under potential load increment. The occurrence of a cascading failure is initiated by removal of a node, which in general changes the distribution of shortest paths. Then the load at a particular node can change and if it increases and exceeds its capacity, the corresponding node fails. Any failure leads to a new redistribution of loads and, as a result, subsequent failures can occur. It should be noted that the single failure mechanism applied here does not attempt to simulate a realistic trigger event of cascading failure; instead, it is only a manner of starting the cascading failure simulation for the ML model (and the OPA model introduced below).

Using this cascading failure model, the vulnerability of network Q can be characterized by the fraction of network efficiency lost in the cascading failure:

$$Vul(Q) = \frac{E(Q) - E(\bar{Q})}{E(Q)} \quad (3)$$

where $Vul(Q) \in (0,1)$ and $\bar{Q}$ represents the residual network structure after the initial failure. $E(Q)$ measures the network efficiency based on the node pair shortest path distance between generators and distributors. For its computation all pairs of nodes $i \in V_G$, and $j \in V_D$ are weighted by the inverse of their distance:

$$E(Q) = \frac{1}{N_G N_D} \sum_{i \in V_G} \sum_{j \in V_D} \frac{1}{d(i,j)} \quad (4)$$

where $d(i,j)$ is the number of edges for an unweighted network or the sum of edge weights for a weighted network in the shortest path from *i* to *j*.

The geodesic vulnerability $Vul(Q)$ measures the functionality of a network when subjected to a contingency due to cascading link disruption with regard to its steady state (base case). As $Vul(Q)$ increases, the impact on the network due to cascading failure also increases, as some components become disrupted. $Vul(Q)$ has been proved to be a well-defined index being capable of providing results consistent with those of physical model indices [26].

The detailed simulation of the ML cascading failure model proceeds as follows:

Step 1. Apply equation (1) to compute the initial load of each node for a proposed network by Floyd's shortest paths algorithm [31] and calculate the capacity of each node based on equation (2).

Step 2. Trigger the initial failure. In the optimization, one of the top five most loaded nodes is chosen and removed from the network.

Step 3. Recur to equation (1) and Floyd's shortest paths algorithm to recalculate the load of each working node in the network.

Step 4. Test each node for failure: for each node k ($k \in N$) of the network, if $L_k > C_k$ then node k is regarded as failed and, thus, is removed from the network.

Step 5. If any working node fails, return back to step 3. Otherwise, terminate the cascading simulation and evaluate the vulnerability of the network using equation (3).

Complex network theory models, such as the ML that we use within our optimization framework in Section 3, have no direct physical relation to the mechanisms of realistic power grids, but they have the key advantage that by utilizing techniques from graph theory they can be applied to analyze large-scale networks. For this reason, this modelling approach is seeing increasing applications for modelling cascading failure processes in power grids.

2.2. The OPA model

The OPA model has been proposed by researchers at Oak Ridge National Laboratory (ORNL), Power System Engineering Research Center of Wisconsin University (PSerc), and Alaska University (Alaska) [10-12]. The OPA model, built upon the Self-Organized Criticality (SOC) theory, contains two interdependent time scale dynamics, i.e., fast power flow dispatching dynamics and slow power grid growth dynamics, to describe the complexity and criticality of power systems. The slow time scale dynamics describes how the system evolves as demand changes over longer timeframes (e.g., over days), and due to subsequent system upgrades in response to demand variations and blackouts. On the other hand, the fast time scale dynamics depicts cascading failures of transmission lines over very short times (e.g., over seconds) during the slow dynamics. It is a novel and powerful tool for analyzing power systems. Our analyses focus on the fast power flow dynamics, in order to ensure comparability with the ML model and its underlying shortest-path assumption.

The cascading failure model is based on the standard DC power flow equation,

$$F = AP \tag{5}$$

where F is a vector whose N_E components are the power flows through the lines, F_{ij} (N_E is the total number of links in the network), P is a vector whose N-1 components are the power injection of each node, P_i (N is the total number of nodes in the network), with the exception of the reference generator, P_0, and A is a constant matrix that depends on the network structure and impedances (see Ref. (11) for

details about the computation of *A*). The reference generator power is not included in the vector *P* to avoid singularity of *A* as a consequence of the overall power balance.

The generator power dispatch is solved using standard linear programming methods. Using the input power demand, the power flow equation (5) is solved with the condition of minimizing the following cost function:

$$Cost = \sum_{i \in V_G} P_i(t) + K \sum_{j \in V_D} P_j(t) \quad (6)$$

where V_G and V_D are the sets of generators and distributors, respectively. This definition gives preference to generation shift whilst assigning a high cost (set K = 100) to load shedding, and it is assumed that all generators operate at the same cost and that all loads are served with equal priority. The minimization is done with the following constraints:

(1) Generator power injections are generally positive and limited by installed capacity limits: $0 \leq P_i \leq P_i^{max}, i \in V_G$.

(2) Loads always have negative power injections: $P_j^{dem} \leq P_j \leq 0, j \in V_D$.

(3) The absolute flow through links is limited by link capacities: $|F_{ij}| \leq F_{max}$.

(4) Total power generation and consumption remain balanced: $\sum_{i \in V_G \cup V_D} P_i = 0$.

After solving the linear optimization by using the simplex method as implemented in Ref. (32), we examine which lines are overloaded. A line is considered to be overloaded if the power flow through it is within 1% of the limit capacity F_{max}. Each overloaded line may outage with probability p_1 (p_1 is set as 1 in the case study to ensure its comparability with ML). If an overloaded line experiences an outage, its power flow limit F_{max} is divided by a very large number k_1 to ensure that practically no power may flow through the line. This action can avoid the infeasibility of the power flow optimization due to topological islands in the system by removing the component directly. Besides, to avoid a matrix singularity from the line outage, the impedances of failed lines are multiplied by a large number k_2, resulting in changes of the network matrix *A*.

Load shedding is utilized to quantify the damage of the cascading failure. For an individual node, load shedding is defined as the difference between its power injection and demand:

$$S_i = P_i^{dem} - P_i \quad (7)$$

Subsequently, total load shedding for the system is:

$$S = \sum_{i \in V_D} S_i \quad (8)$$

Finally, system load shedding is normalized by its total demand *D* and used as a measure of cascading vulnerability:

$$S/_D = \frac{\sum_{i \in V_D} S_i}{\sum_{i \in V_D} P_i^{dem}} \quad (9)$$

The fact that simulation results from OPA model are consistent with historical blackout data for real power systems has justified its effectiveness [12]. However, the applications of OPA have generally been limited to networks with a relatively small number of nodes compared to real power grids [24], due to the computational efforts involved.

3 OPTIMIZATION MODEL

For a given network, cascading failure resilience could be enhanced in many ways. In this paper, we focus on choosing the connecting patterns between generators and distributors of a realistic power transmission network, so as to optimize resilience to cascading failures. In this study, system vulnerability to cascading failures (i.e. system functionality loss in cascading failures) is regarded as a reverse measure of system resilience: the less the functionality loss, the higher the system resilience. Given the goal of analyzing a realistic-size network, the ML cascading failure model is used to evaluate the resilience of a pattern of connections. By associating a cost to each link posed in the network, the optimization also seeks to minimize the total cost.

The network is modeled as a weighted graph, in which the edge weights are given by their physical distances which we assume directly related to the transmitting cost of the link. We define the variables to be optimized as the links of generation nodes to the different distribution nodes:

$$X_{ij} = \begin{cases} 1, \text{if } i \text{ is connected with } j \text{ directly} \\ 0, \text{otherwise} \end{cases} \quad (10)$$

for all $i \in V_G$ and $j \in V_D$. Two constraints have to be met when rewiring generators and distributors: (1) each distributor node is required to connect with at least one generator node or other distributor node, to make it accessible to the power supplying generators; (2) each generator node has to connect at least with one distributor node.

We assume that the cost associated with each connection cutting and rewiring is linearly proportional to the physical length of the linkage, with coefficient φ. The total investment cost of a reconstructed pattern X in the power transmission network can be defined as

$$C = \sum_{i \in V_G} \sum_{j \in V_D} \varphi X_{ij}\, d(i,j) \quad (11)$$

where $d(i,j)$ is the physical distance between i and j.

The cascading failure resilience of each reconstructed pattern X can be quantified by the vulnerability of the new network, given by equation (3). It should be noted that the effect of the type of initial event could significantly influence the cascading failure result: the efficiency loss of a cascade triggered by

the failure of a critical component could be much more severe than that originated by the failure of a normal component. Therefore, we consider a worst-case scenario in this study by choosing the failure of one of the top five most loaded nodes as initial failure in each cascade process simulation and, then, the results are averaged on the number of simulations.

Through the quantification of the connection pattern cost and cascading failure vulnerability, the facility allocation problem is formulated as a multi-objective optimization problem:

$$\begin{cases} \min C(X_{ij}) & (12a) \\ \min Vul\left(Q_{X_{ij}}\right) & (12b) \end{cases}$$

$$s.t. \begin{cases} \sum_{i \in V_G \cup V_D} X_{ij} > 0 \ \forall j \in V_D & (12c) \\ \sum_{j \in V_D} X_{ij} > 0 \ \forall i \in V_G & (12d) \end{cases}$$

The objective function (12a) is the sum of the fixed rewiring costs; (12b) expresses the resilience objective. The two constraints mentioned above are enforced by formulas (12c) and (12d), respectively. Observe that the least costly generator allocation is simply that with no links among facilities and consumers.

In our work, the multi-objective optimization problem (12a) – (12d) is tackled by the Non-dominated Sorting Binary Differential Evolution (NSBDE) algorithm presented in the next Section 4.

4 NON-DOMINATED SORTING BINARY DIFFERENTIAL EVOLUTION ALGORITHM FOR TOPOLOGY OPTIMIZATION

In this section, the operative procedures of the Non-dominated Sorting Binary Differential Evolution (NSBDE) algorithm are proposed for solving the multi-objective optimization problem introduced in Section 3 above. The starting point is the standard Differential Evolution (DE) algorithm, initially proposed as a population-based global optimization method for real-valued optimization problems, which has been found to outperform other optimization algorithms in various applications [21, 33, 34]. In order to solve the combinatorial multi-objective problem of interest, the fast non-dominated sorting, ranking and elitism techniques used in non-dominated sorting genetic algorithm-II (NSGA-II) [35] are introduced into a modified binary differential evolution (MBDE), which is a binary version of DE developed to tackle single-objective binary-coded optimization problems [36]. The NSBDE proceeds as follows: [21]

Step 1. Initialization of parameters

Set the values of the population size *NP*, the crossover rate *CR*, the scaling factor *F*, and the maximum generations N_{max}.

Step 2. Generation of initial population and evaluation

Initialize each individual in the population which is represented as a bit-string and denoted as $px_i^t = \{px_{ij}^t, |px_{ij}^t \in \{0,1\}; i = 1,2,\dots,NP, j = 1,2,\dots,M\}$, where *NP* is the population size and *M* is the dimensionality of the solutions. Each individual is also called a chromosome and forms a candidate solution to the problem. Each bit of each initial chromosome takes a value from the set {0, 1} with probability equals to 0.5: the bit takes '1' if the corresponding generator node and distributor node are connected, '0' otherwise.

Each of the *NP* chromosomes is evaluated by computing the two objective functions, i.e. formula (12a) and (12b).

Step 3. Generation of trial population

Apply the binary tournament selection operator [35] to the population PX^t to generate a trial population PV^t, which undergoes the evolution operations of mutation and crossover.

Step 3.1 Mutation

The following probability estimation operator *P*(*px*) is utilized to generate the mutated individuals according to the information of the parent population:

$$P\left(px_{ij}^t\right) = \frac{1}{1+e^{-\frac{2b[px_{r1,j}^t + F\left(px_{r2,j}^t - px_{r3,j}^t\right) - 0.5]}{1+2F}}} \tag{13}$$

where *b* is a positive real constant, usually set as 6; *F* is the scaling factor; $px_{r1,j}^t$, $px_{r2,j}^t$ and $px_{r3,j}^t$ are the *j*-th bits of three randomly chosen individuals at generation *t*. According to the probability estimation vector $P\left(px_i^t\right) = [px_{i,1}^t, px_{i,2}^t, \dots\ px_{i,N}^t]$ created by equation (13), the corresponding offspring pu_i^t of the current target individual px_i^t is generated as equation (14).

$$pu_{ij}^t = \begin{cases} 1, & \text{if } rand \le P(px_{ij}^t) \\ 0, & \text{otherwise} \end{cases} \tag{14}$$

where *rand* is a uniformly distributed random number within the interval [0,1].

Step 3.2 Crossover

The crossover operator is used to mix the target individual and its mutated individual. The trial individual $pv_{ij}^t = (pv_{i,1}^t, pv_{i,2}^t, \dots\ pv_{i,N}^t)$ can be obtained by the crossover operator as follows,

$$pv_{ij}^t = \begin{cases} pu_{ij}^t, & \text{if } randj \le CR \text{ or } j = randi \\ px_{ij}^t, & \text{otherwise} \end{cases} \tag{15}$$

where *randj* $\in (0,1]$ is a uniform random value, *CR* is the crossover rate, and *randi* is a uniform discrete random number in the set {1, 2, ..., *NP*}.

Step 4. Evaluation

Evaluate each of the *NP* chromosomes in the population PV^t by computing its rewiring cost (12a) and resilience to cascading failures (12b) by performing the ML cascade process simulation procedure presented in Section 2.2.

Step 5. Union and Sorting

Combine the parent and trial populations to obtain a union population $PU^t = PX^t \cup PV^t$. Rank the individuals in the union population by the fast non-dominated sorting algorithm [33] with respect to the objective values, and identify the ranked non-dominated fronts F_1, F_2, …, F_k where F_1 is the best front, F_2 is the second best front and F_k the least good front.

Step 6. Selection

Select the first *NP* individuals from PU^t to create a new parent population PX^{t+1}. The crowding distance is used in this step to choose the individuals with the same front, where crowing refers to the density of solution present in a neighborhood of an individual of specified radius [35]: we prefer the individual which is located in a region with least number of individuals. The algorithm stops when it reaches the predefined maximum generations N_{max}.

5 CASE STUDY AND RESULTS ANALYSIS

5.1. Case study and parameters setting

In this paper, the 400kV French power transmission network (FPTN400) (Figure 1) is taken for exemplification of the proposed approach. The network is built from the data on the 400 kV transmission lines of the RTE website [37]. It has 171 nodes (substations) and 220 edges (transmission lines). We distinguish the generators, which are the source of power, from the other distribution substations, that receive power and transmit it to other substations or distribute it in local distribution grids. By obtaining the power plants list from EDF website [38] and relating them with the ID of the buses in the transmission network, we have 26 generators and 145 distributors. Only the nuclear power plants, hydroelectric plants and thermal power plants whose installed capacities are larger than 1000 MW, are considered.

For reallocation of the power generating nodes to the other nodes, the NSBDE algorithm introduced in the previous section is applied. The parameters values used to run the NSBDE algorithm are reported in Table I. The tuning parameters are chosen based on trial-and-improvement for fast convergence of the algorithm [28]. The network tolerance parameter α is set to 0.3 to simulate the normal operating condition; linkage cost parameter φ is set to 1.

Fig. 1. The 400kV French power transmission network (FPTN400) [37]

At the beginning of the simulation, all 55 links among generators and distributors in the FPTN400 are cut off. The population is initialized by randomly assigning 0 or 1 to each bit of each chromosome in the population, forming a group of potential rewiring solutions. For evaluating the cascading vulnerability of a given generators-distributors allocation pattern, the ML cascading failure model is run starting from failing one of the top five most loaded (largest betweenness) nodes in repeated cascading simulations at the end of which the vulnerability values are averaged.

Table I . Parameters of the NSBDE algorithm

Parameters	Values
Population size *NP*	25
Dimensionality of solution *M*	3770
Crossover rate *CR*	0.9
Scaling factor *F*	0.2
Maximum generation N_{max}	300

5.2. Topological optimization results

Figure 2 reports the convergence plots of one run of the NSBDE algorithm. The top and bottom panels show the two optimal solutions with regard to the two objectives (12a) and (12b), respectively. It is observed that the algorithm is able to converge after around 150 generations.

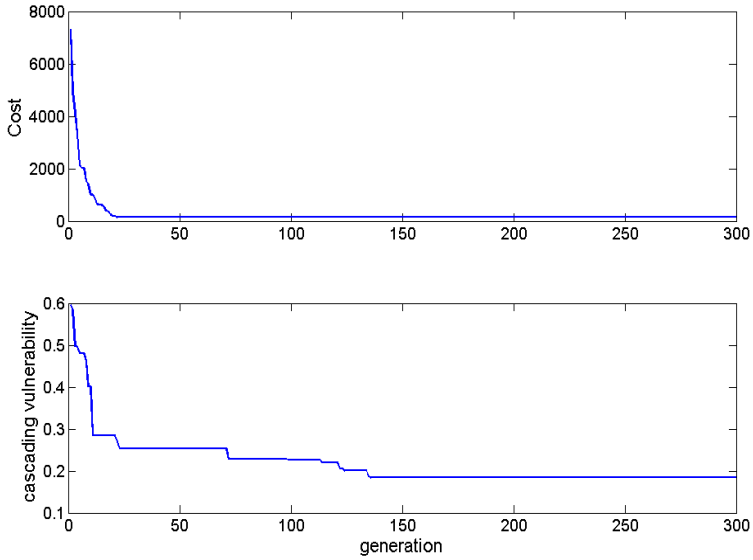


Fig. 2. Convergence plots of objective functions (12a) (top) and (12b) (bottom) during the evolution of NSBDE

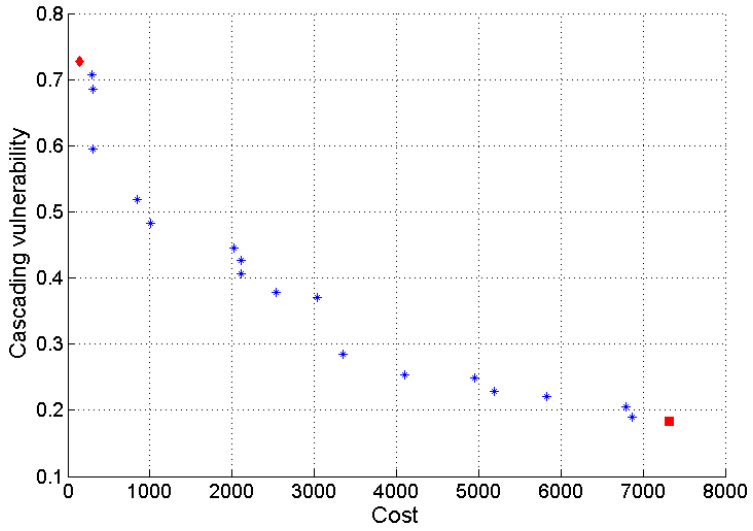


Fig. 3. Pareto front reached by a population of 25 chromosomes evolving for 300 generations

The Pareto front obtained by the NSBDE algorithm at convergence is illustrated in Figure 3. The diamond point in Figure 3 represents the current network with the present pattern of connecting links, which is also the least costly network; the square point is the most resilient network, whose cascading vulnerability is 0.184. It is not unexpected that the original network is the least costly one, since the electrical transmission lines and substations are placed with geographical constraints and connections between two distant substations are avoided. Actually, cost-effectiveness is a major consideration in constructing real power transmission networks.

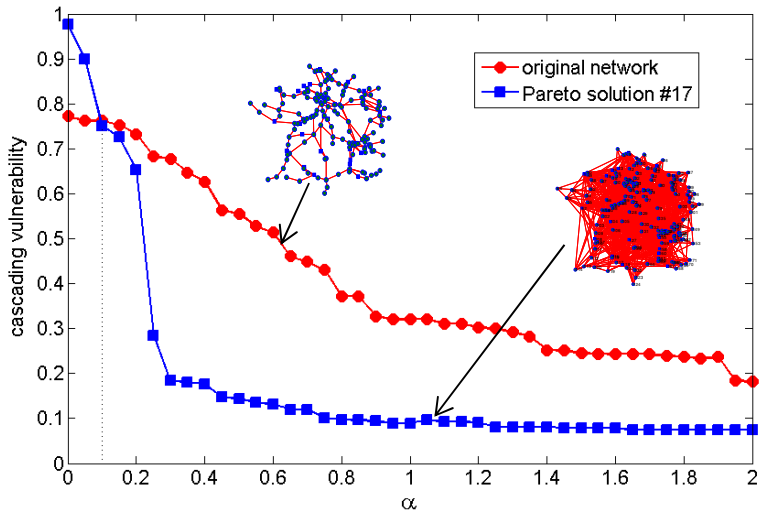


Fig. 4. Comparison of the cascading vulnerability between the original and the most resilient networks under different network tolerance values

It is also noted from Figure 3 that the cascading failure resilience of the FPTN400 can be improved significantly by properly rewiring the generator-distributor connections, though at a cost; the network vulnerability is decreased from 0.728 to 0.184 (when α=1.3) with an increased cost of 7.3×10^3 (i.e., 53.16 times increase). Figure 4 reports the cascading vulnerability comparison between the original network and the most resilient one (Pareto solution #17) with different tolerance parameters. It shows that when the network tolerance is very low, i.e. $0< \alpha < 0.1$, the optimized network loses most of its efficiency, i.e., it is quite vulnerable to intentional attacks possibly due to its intensive loading condition. However, when $\alpha \geqslant 0.3$ (which is generally the normal operating condition [13]), the optimized network loses less than 20% of its efficiency during a cascading failure initiated by intentional attack.

Albeit a substantial improvement of the cascading failure resilience of the FPTN400 is possible by adding redundant links, a tradeoff between the cost and resilience improvement is necessary for rational decision-making. Along the Pareto frontier of the potential solutions, there are some points at which a small sacrifice of cost gives a large gain of cascading resilience. More generally, by taking a network solution and its neighbor on the frontier (the less costly one), one can define a rate of change of cascading resilience with respect to cost: $|\Delta Vul/\Delta cost|$. This rate can be utilized as a reference to choose the optimized network: the larger the ratio, the more preferred the network is.

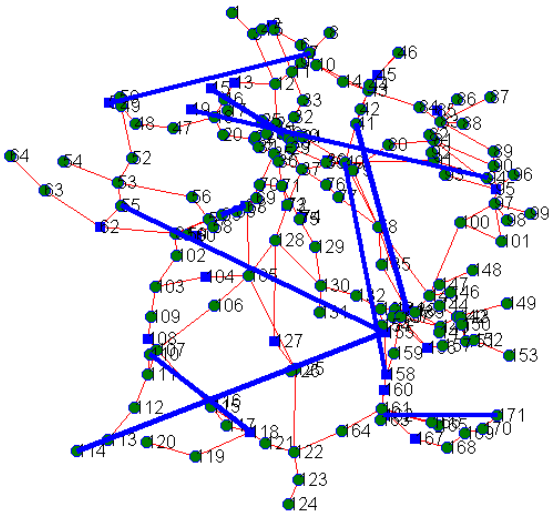


Fig. 5. The topology of the Pareto solution #3 and its difference with the original network

Figure 5 reports the topology of the network corresponding to the Pareto solution #3 (310.6, 0.59) whose $|\Delta Vul/\Delta cost|$ value is comparatively large. The bold links represent the 10 added connections with respect to the original real network: notice that only 10 links are required to be rewired for the original network to gain a 19.2% cascading resilience improvement (the cascading vulnerability is decreased from 0.73 to 0.59). Besides, it is noted from Figure 5 that the newly added links tend to connect distant generator and distributor pairs, indicating that the installation of power lines between remote power substations can improve the resilience of the system, although at larger costs.

5.3. Validation by the OPA model

All the optimization results presented in the previous section are based on the ML model which abstracts basic power flow constraints and electrical characteristics of the power transmission network. In this section, the more realistic OPA model introduced in Section 2.2 is utilized to verify the optimal results found.

The verification is not straightforward due to the differences of the two models in the way of representing system capacity, in the iterative algorithms they rely on, and in the way of measuring the damage produced by the cascading failure. Accordingly, some assumptions and adjustments to the OPA model (as described in Section 5.3.1) are necessary to ensure its applicability to assess the optimization solutions obtained based on the ML model [27].

5.3.1 *OPA Adjustments*

Five representative solutions (i.e., the least cost network FPTN400, the Pareto solution #17 (7300, 0.184) which is the most resilient, together with the solutions #3 (310.6, 0.59), #5 (3344.3, 0.28) and #13 (1003.8, 0.48) whose $|\Delta Vul/\Delta cost|$ values are comparatively large) along the Pareto front are chosen as the basic network topologies to be verified by the OPA model. To facilitate comparability with the ML model, all the generators are assumed to have equal capacity, and all the loads are

assumed to have equal constant demand (we use 26, i.e. the number of generators in the simulation). Furthermore, all edge impedances are calculated using the typical reactance value 0.28 ohm/km at 50 Hz [39]. This heterogeneous impedance setting aligns with the weighted edge initialization in the ML model.

The ML model uses the parameter α to represent network tolerance, while regarding the OPA model, prior studies set the initial limits (demand, generator capacity, line flow limits) by evolving the network using combined fast-slow dynamics until the network reaches a steady state [11]. Considering that we limit the scope of the OPA evaluation to fast dynamics, we use a simpler initialization strategy (proposed by Cupac et al. [27]) which does not require the slow power grid growth dynamics, and apply the parallel capacity setting (the α model) to facilitate the comparison. In particular, the values of the initial flows $\overline{F_{ij}}(0)$ and of the link capacities F_{ij}^{max} are determined as follows: demand for all distributor nodes is fixed to a constant amount, as mention above, and total generation capacity is set to be equal to total demand, and equally divided among the generators. Then, the power flows along the lines are estimated by assuming that every distributor node would obtain an equal amount of power from every generator. The initial flows are calculated by selecting a generator (one at a time), setting all other generator capacities to 0 and then computing power flows to each distributor node. The sum of the power flows over all the generators results in the estimated initial flow along each link, $\overline{F_{ij}}(0)$. Analogous to the initialization process in the ML model, the maximum capacity for a link connecting nodes *i* and *j* is given by

$$F_{ij}^{max} = (1 + \alpha)\left|\overline{F_{ij}}(0)\right| \tag{16}$$

It is noted that the values of the initial flows $\overline{F_{ij}}(0)$ are only used to set the link flow capacities F_{ij}^{max} in such a way that they are comparable to the capacities C_k used by the ML model. The network tolerance parameter is set to $0 \leq \alpha \leq 2$ in our approach, parallel to the ML model, representing excess transmission capacity. Then, the node transmission capacity is modelled as the sum of link flow capacities of adjacent links $\sum_{j \in V_j} F_{ij}^{max}$ where V_j is the set of nodes directly connected to node *i*.

In the OPA implementation, the probability of an overloaded link is set to $p_1 = 1$ (identical with that in Cupac et al. [27]), to ensure comparability with ML, where an overloaded node fails and is removed from the network with certainty. This setting will not change the OPA validation results where only the relative ranking of cascade vulnerability for each network is considered, although it has probably changed all the absolute values of cascade vulnerability. Besides, we initiate the cascade in the same manner that we do in the ML model, as stated in Section 3.

5.3.2 *Validation Results*

Figure 6 reports the landscapes of the node transmission capacities C_k and F_{ij}^{max} under both ML model and OPA model, respectively, for the five chosen networks (with $\alpha = 0$). It shows that node capacities in ML are highly correlated with node capacities in OPA model for the FPTN400, Pareto solution #3, #5 and #13 (actually, the correlation coefficients are 0.904, 0.890, 0.862 and 0.914 respectively); for Pareto solution #17, the linear correlation of node transmission capacities still exists (with correlation coefficient 0.619). This indicates that the initialization strategy is consistent for ML and OPA models: nodes with high capacity in ML tend to have high capacity in OPA, and nodes with low capacity in ML also tend to have low capacity in OPA [27].

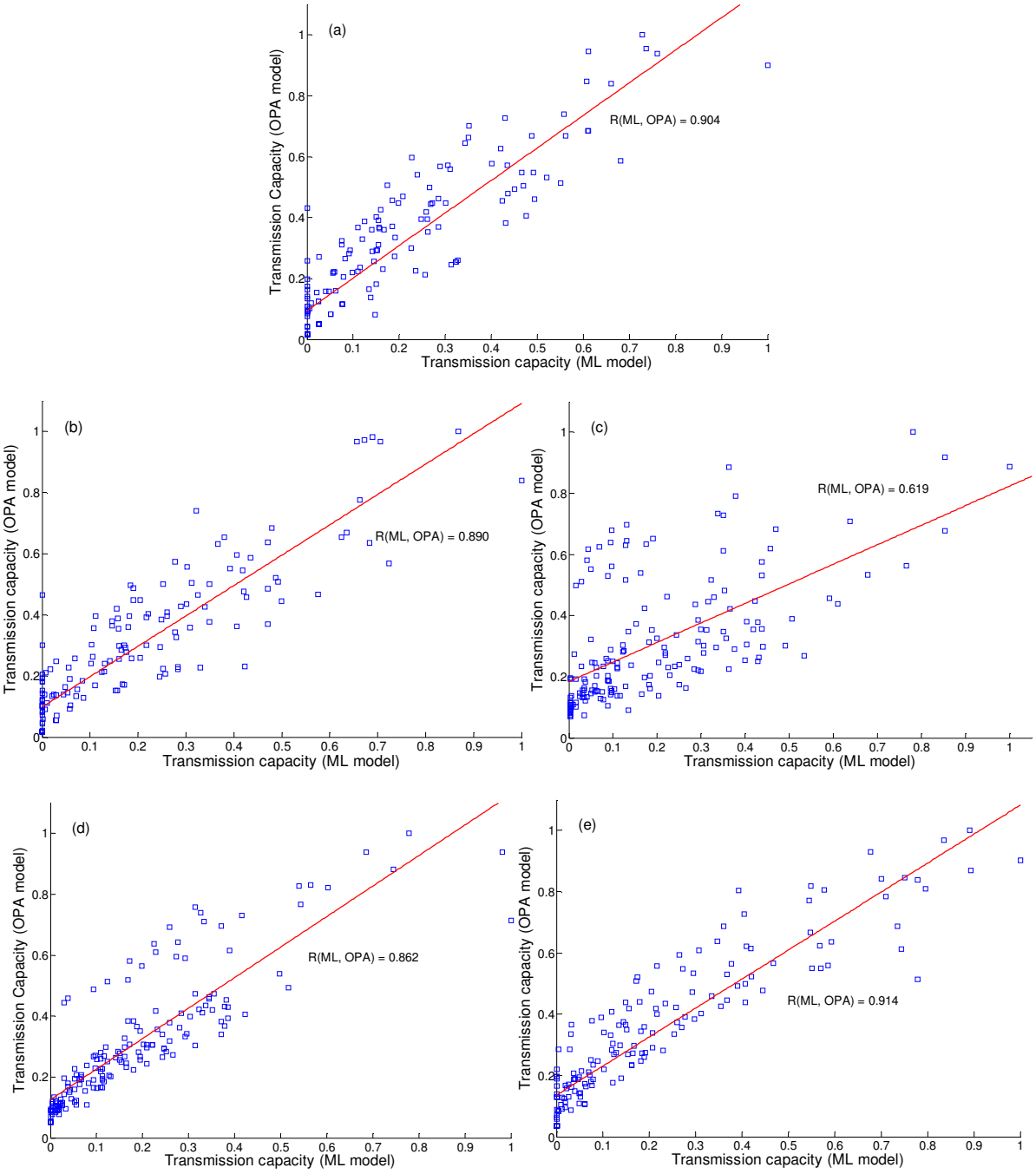


Fig. 6. Scatterplot of normalized node transmission capacity in ML versus OPA model using, (a) the original FPTN400; (b) Pareto solution #3 network; (c) Pareto solution #17 network; (d) Pareto solution #5; (e) Pareto solution #13. Node transmission capacity in OPA is highly correlated with transmission capacity in ML, the correlation coefficient are 0.904, 0.890, 0.619, 0.862 and 0.914 for the five networks, respectively. The solid lines represent the best fits.

In Figure 7, we plot the curves of normalized load shedding S/D versus network tolerance α obtained by applying the OPA model to the five representative networks selected from the Pareto front. The OPA simulation is triggered by removing one of the top five most loaded nodes (i.e., targeted initial failure). Analogous to the ML model (Figure 4), the network damages decreases when network tolerance increases for all the networks. When network tolerance value is high enough ($\alpha > 1.2$), any small intentional disturbance on the network would tend to cause quite low damage to the functioning of the network ($< 1\%$). Most importantly, it is observed that in the OPA simulation, the network corresponding to Pareto solution #3 (310.6, 0.59) (green triangle curve) is more resilient, i.e., it presents less load shedding than the original network (red circle curve) over a wide range of network tolerance α (i.e., $0 < \alpha < 1.2$); in addition, solution #13 (1003.8, 0.48) (magenta diamond curve) generally outperforms the solution #3, while solution #5 (3344.3, 0.28) (grey star curve) outperforms #13 in terms of cascade resilience. Finally, Pareto solution #17 (7300, 0.184) (which is the most resilient network according to the ML model) presents the lowest load shedding among the five networks over the entire range of α values considered. This ranking of cascading failure resilience is consistent with the simulation results based on ML model.

Figure 8 shows the results of OPA simulation on the five networks, where the failures are triggered by removing a randomly chosen node (i.e., random initial failure) and the results are averaged over 30 different samples. The ranking of cascade resilience of the five networks here is also parallel with the optimization results based on ML. This demonstrates that a resilience-improved network from the optimization based on the ML model is also more resilient than another one if evaluated by the more realistic OPA cascade simulation, therefore, verifying that the insights gained by the topological optimization approach are valid.

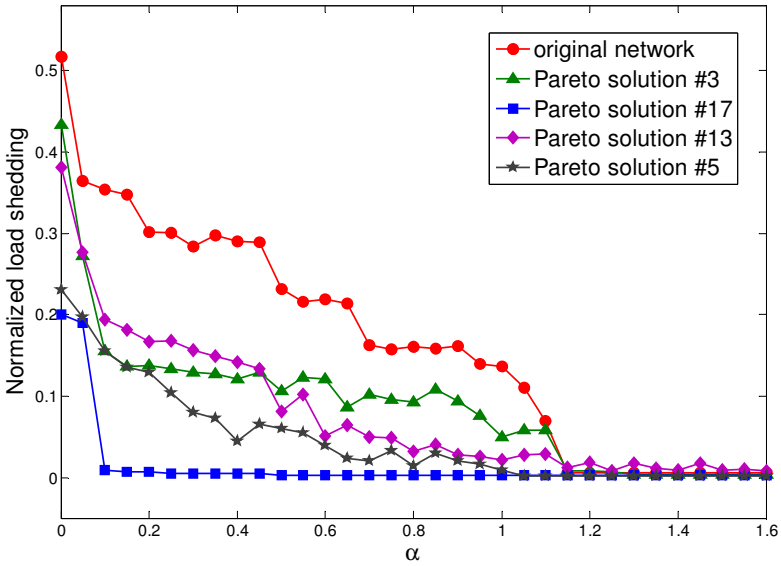


Fig. 7. Cascading vulnerability (normalized load shedding) evaluated by the OPA model for the five chosen networks over a range of network tolerance values α under targeted initial failure.

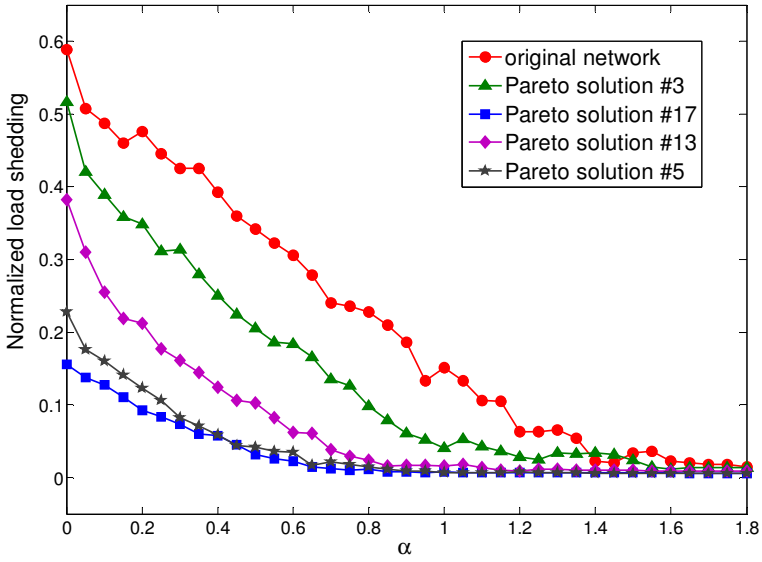


Fig. 8. Cascading vulnerability (normalized load shedding) evaluated by the OPA model for the five chosen networks over a range of network tolerance values α under random initial failure. The results have been averaged over 30 different samples.

Also important is to remember that the results produced by the simple ML topological model are obtained at a much lower computational cost than those of the OPA model: actually, the average time needed to carry out a single cascading failure simulation is 3.9s and 20.8s for the ML and OPA models, respectively, on a double 2.4 GHz Intel CPU and 4 GB RAM computer.

6 DISCUSSION AND CONCLUSIONS

Generally, the structure of power grids emerges through an unplanned growth process to meet service demand and/or results from optimization of costs. However, the increasing threat of large scale

failures, albeit infrequent, makes it vital to think of the design of resilient network systems capable to resist against and recover from cascading failures.

In this paper, we have investigated the allocation of generators to distributor nodes by rewiring links under the objectives of maximizing the network cascading failure resilience and minimizing the investment costs.

In realistic cases of networks of large number of nodes, the problem is a combinatorial multi-objective optimization problem. To effectively tackle the problem, we have proposed a NSBDE multi-objective algorithm, within a Pareto optimality scheme of search for non-dominated solutions. To simulate and quantify the cascading failure resilience of network connection solutions selected during the NSBDE search, a complex network model – namely, the Motter-Lai (ML) model – has been used, to exploit is rapidity of calculation.

Exemplification has been done by considering the 400kV French power transmission network (FPTN400). The results of the case study have shown that generator-distributor allocation can be optimized to improve the cascading resilience of a realistic power transmission network system at an acceptable cost.

To validate the physical significance of the topological optimization results, a detailed and more realistic power flow model – i.e., the ORNL-Pserc-Alaska (OPA) model – has been considered. The OPA model has been applied to five network topologies selected from the Pareto front found by the topological optimization process. The ranking of the five selected networks with respect to their vulnerability to both intentional attacks and random failure is consistent with that of the ML model; in addition, the computational time required by the ML approach is shown to be 5.5 times lower than that of the OPA approach. This verifies (i) the physical meaningfulness of the topological optimization solutions and (ii) the practical usefulness of abstract cascading models in network optimization tasks.

It is noted that this consistency is not insignificant since it demonstrates that one resilience-improved pattern of capacity allocation optimized by the ML model is also of higher resilience if measured by the more realistic OPA model, providing motivation for the use of topological, complex network theory models for ensemble analysis and optimization of large infrastructures against cascading failure with the advantages of simplicity, scalability and low computational cost (e.g., future studies may consider using complex network cascading models to optimize both the topology and electrical/reliability properties of realistic power networks, which may enable unraveling questions such as which type of resource distribution is the most favorable for a network to resist to cascading failures, when the total resource is limited).

The initialization strategy of the OPA model in this paper ensures that we can use the network tolerance parameter α as a common measure of transmission capacity for both models. However, the

actual data could be used in the OPA validation if they are initially applied in the optimization based on the ML model, and if they are available. This could be possible future work. Besides, performing optimizations using directly detailed and computationally intensive power flow models (e.g., embrace Newton-Raphson based power flow approaches [45] and/or realistic trigger events such as natural hazard and malevolent targeted disruption [46], into the cascade modelling framework) would enable a more thorough and comprehensive comparison of the two classes of approaches considered in this paper. Furthermore, it may be useful to model variations in generation capacity and to consider situations where generation capacity and demand are not equally distributed, which is aligned with more realistic cases of power grids. Finally, while being relatively small compared to real scenarios with thousand buses due to computational constraints and data availability, the proposed network is sufficient to illustrate the usefulness of the topological optimization methodology in this study. Nevertheless, we believe that application of the topological approach to large-scale networks is interesting and this falls perfectly within the scope of our future research in this direction.

REFERENCES

(1) Final Report on the August 14, 2003 Blackout in the United States and Canada, US-Canada Power System Outrage Task Force, Tech. Rep., 2004.
(2) Final Report System Disturbance on 4 Nov. 2006, Union for the Coordination of Transmission of Electricity, Tech. Rep., 2007.
(3) Helen Pidd. India blackouts leave 700 million without power. The Guardian, 31 July 2012.
(4) Battiston, Stefano, et al. Credit chains and bankruptcy propagation in production networks. Journal of Economic Dynamics and Control 31.6 (2007): 2061-2084.
(5) Newman, Mark EJ, et al. Email networks and the spread of computer viruses. Physical Review E 66.3 (2002): 035101.
(6) Zhao Kang, et al. Analyzing the resilience of complex supply network topologies against random and targeted disruptions. Systems Journal, IEEE 5.1 (2011): 28-39.
(7) Kempe, David, Jon Kleinberg, and Éva Tardos. Maximizing the spread of influence through a social network. Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, ACM, 2003.
(8) Motter AE, Y-C Lai. Cascade-based attacks on complex networks. Physical Review E 66.6 (2002): 065102.
(9) Crucitti, Paolo, Vito Latora, and Massimo Marchiori. A model for cascading failures in complex networks. Physical Review E 69.4 (2004): 045104.
(10) Dobson Ian, et al. Complex systems analysis of series of blackouts: cascading failure, criticality, and self-organization. Bulk power system dynamics and control-VI (2004): 22-27.
(11) Dobson I, Carreras BA, Lynch VE, Newman DE. An initial model for complex dynamics in electric power system blackouts. In: Proceedings of the 34th annual Hawaii international conference on system sciences, 2001; 2001. p. 710–8.
(12) Carreras BA, Newman DE, Dobson I, and Poole AB. Evidence for self-organized criticality in a time series of electric power system blackouts. Circuits and Systems I: Regular Papers, IEEE Transactions on 51, no. 9 (2004): 1733-1740.
(13) Baldick R, et al. Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures. Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, pp. 1-8.
(14) Albert, Réka, István Albert, Gary L. Nakarado. Structural vulnerability of the North American power grid. Physical Review E 69.2 (2004): 025103.
(15) Thadakamaila, HP, et al. Survivability of multiagent-based supply networks: a topological perspective. Intelligent Systems, IEEE 19.5 (2004): 24-31.
(16) Boorstyn, Robert, Howard Frank. Large-scale network topological optimization. Communications, IEEE Transactions on 25.1 (1977): 29-47.

(17) Shao, Fang-Ming, Xuemin Shen, Pin-Han Ho. Reliability optimization of distributed access networks with constrained total cost. Reliability, IEEE Transactions on 54.3 (2005): 421-430.
(18) Gutfraind A. Optimizing topological cascade resilience based on the structure of terrorist networks. PloS one 5.11 (2010): e13448.
(19) Newth, David, Jeff Ash. Evolving cascading failure resilience in complex networks. Proc. of 8th Asia Pacific Symp. on Intelligent and Evolutionary Systems. 2004.
(20) Cadini, F., Zio, E., & Petrescu, C. A. (2010). Optimal expansion of an existing electrical power transmission network by multi-objective genetic algorithms. Reliability Engineering & System Safety, 95(3), 173-181.
(21) Li Y-F, Sansavini G, Zio E. Non-Dominated Sorting Binary Differential Evolution for the Multi Objective Optimization of Cascading Failures Protection in Complex Networks. Reliability Engineering & System Safety (2012).
(22) Zio E., Golea LR, Sansavini G. Optimizing protections against cascades in network systems: A modified binary differential evolution algorithm. Reliability Engineering & System Safety, Volume 103, July 2012, Pages 72-83.
(23) Kinney R, Crucitti P, Albert R, & Latora V. Modeling cascading failures in the North American power grid. The European Physical Journal B-Condensed Matter and Complex Systems, 46.1(2005): 101-107.
(24) Sun K, Han Z-X. Analysis and comparison on several kinds of models of cascading failure in power system. In: Transmission and distribution conference and exhibition: Asia and Pacific, 2005 IEEE/PES; 2005. p. 1–7.
(25) Buldyrev, Sergey V, et al. Catastrophic cascade of failures in interdependent networks. Nature 464.7291 (2010): 1025-1028.
(26) Correa GJ, and Yusta JM. Grid vulnerability analysis based on scale-free graphs versus power flow models. Electric Power Systems Research 101 (2013): 71-79.
(27) Cupac V, Lizier JT, Prokopenko M. Comparing dynamics of cascading failures between network-centric and power flow models. International Journal of Electrical Power & Energy Systems, 49, (2013): 369-379.
(28) Fang, YP, Pedroni, N. and Zio, E. Optimal Production Facility Allocation for Failure Resilient Critical Infrastructures. In ESREL 2013 (2013, September).
(29) Purchala K, Meeus L, Van Dommelen D, Belmans R. Usefulness of DC power flow for active power flow analysis. In Power Engineering Society General Meeting, 2005. IEEE (pp. 454-459). IEEE. (2005, June).
(30) Holmgren AJ. Using graph models to analyze the vulnerability of electric power networks. Risk analysis 26.4 (2006): 955-969.
(31) Floyd RW. Algorithm 97: shortest path. Communications of the ACM 5.6 (1962): 345.
(32) Press WH, Flannery BP, Teukolsky SA, Vetterling WT. Numerical Recipes in C. Cambridge Unversity Press, Cambridge, 1988.
(33) Price KV, Storn RM, Lampinen JA. Differential evolution a practical approach to global optimization. (2005).
(34) Ponsich A, Coello CA. Differential Evolution performances for the solution of mixed-integer constrained process engineering problems. Applied Soft Computing, 11.1(2011): 399-409.
(35) Deb Kalyanmoy, et al. A fast and elitist multiobjective genetic algorithm: NSGA-II. Evolutionary Computation, IEEE Transactions on 6.2 (2002): 182-197.
(36) Wang Ling, et al. A modified binary differential evolution algorithm. Life System Modeling and Intelligent Computing. Springer Berlin Heidelberg, 2010. 49-57.
(37) RTE. Le Réseau de Transport d'Electricité 400 kV, 2011, http://www.rte-france.com
(38) EDF. En direct de nos centrales, http://france.edf.com/france-45634.html, Retrieved Avril, 2013.
(39) Zhou Q, Bialek JW. Approximate model of European interconnected system as a benchmark system to study effects of cross-border trades. Power Systems, IEEE Transactions on, 20.2 (2005): 782-788.
(40) Fitzmaurice R, Cotilla-Sanchez E, Hines P. Evaluating the impact of modeling assumptions for cascading failure simulation. In Power and Energy Society General Meeting, 2012 IEEE (pp. 1-8). IEEE.
(41) Hines P, Cotilla-Sanchez E, Blumsack S. Do topological models provide good information about electricity infrastructure vulnerability? Chaos: An Interdisciplinary Journal of Nonlinear Science, 20.3 (2010), 033122.
(42) Cotilla-Sanchez E, Hines PD, Barrows C., Blumsack S. Comparing the topological and electrical structure of the North American electric power infrastructure. Systems Journal, IEEE, 6.4 (2012), 616-626.

(43) Dobson I, Carreras BA, Newman DE. A loading-dependent model of probabilistic cascading failure. Probability in the Engineering and Informational Sciences, 19.1 (2005), 15-32.
(44) Leelaruji R, Valerijs K. Modeling adequacy for cascading failure analysis. In Power Engineering Conference, 2008. AUPEC'08. Australasian Universities, pp. 1-6. IEEE, 2008.
(45) Wang H, and Thorp JS. Optimal locations for protection system enhancement: a simulation of cascading outages. Power Delivery, IEEE Transactions on, 16(4), pp. 528-533, 2001.
(46) Dueñas-Osorio L, Vemuru SM. Cascading failures in complex infrastructure systems. Structural safety, (2009) 31(2), 157-167.

Paper [4] Y.-P. Fang, N. Pedroni, E. Zio. "Comparing network-centric and power flow models for the optimal allocation of link capacities in a cascade-resilient power transmission network." IEEE System Journal, vol.PP, no.99, pp.1, 12, 2014.

Comparing Network-Centric and Power Flow Models for the Optimal Allocation of Link Capacities in a Cascade-Resilient Power Transmission Network

Y.-P. Fang, N. Pedroni, E. Zio, *Senior Member*, *IEEE*

***Abstract*—In this study, we tackle the problem of searching for the most favourable pattern of link capacities allocation that makes a power transmission network resilient to cascading failures with limited investment costs. This problem is formulated within a combinatorial multi-objective optimization framework and tackled by evolutionary algorithms. Two different models of increasing complexity are used to simulate cascading failures in a network and to quantify its resilience: a complex network model (namely, the Motter-Lai (ML) model) and a more detailed and computationally demanding power flow model (namely, the ORNL-Pserc-Alaska (OPA) model). Both models are tested and compared on a case study involving the 400kV French power transmission network. The results show that cascade-resilient networks tend to have a non-linear capacity-load relation: in particular, heavily loaded components have smaller unoccupied portions of capacity, whereas lightly loaded links present larger unoccupied portions of capacity (which is in contrast with the linear capacity-load relation hypothesized in previous works of literature). Most importantly, the optimal solutions obtained using the ML and OPA models exhibit consistent characteristics in terms of phrase transitions in the Pareto fronts and link capacity allocation patterns. These results provide incentive for the use of computationally-cheap network-centric models for the optimization of cascade-resilient power network systems, given the advantages of their simplicity and scalability.**

***Index Terms*—power transmission network, cascading failures, complex network theory model, power flow model, capacity optimization, evolutionary algorithm**

I. Introduction

OUR modern society has come to depend on large-scale critical infrastructures (CIs) to deliver resources and services to consumers and businesses in an efficient manner. These CIs are complex networks of interconnected functional and structural elements. Large scale outages on these real-world complex networks, although infrequent, are increasingly disastrous to our society, with estimates of direct costs up to billions of dollars and inestimable indirect costs. Typical examples include blackouts in power transmission networks [1]-[3], financial bankruptcy [4], telecommunication outages [5], and catastrophic failures in socio-economic systems [6], [7].

Research regarding modelling, prediction and mitigation of cascading failures in CIs, whereby small initial disturbances may propagate through the whole infrastructure system, has addressed the problem in different ways, including physical models for describing cascading failure phenomena [8]-[11], control and defense strategies against cascading failures [12]-[14], analytical calculation of capacity parameters [15], and modelling of the real-world data [16].

In particular, various problems concerning the robustness and functionality of CI systems (ranging from power outages and Internet congestion to affordability of public transportation) are ultimately determined by the extent to which the CI capability matches supply and demand under realistic conditions [17]. In this respect, the following two issues are closely related to each other and of significant interests: (i) how to improve the network resilience to cascading failures, and (ii) how to design CI systems with a reasonably limited cost. In most circumstances, high resilience and low cost are conflicting objectives and cannot be achieved simultaneously. For instance, a network whose components have high capacity can be highly resilient to failures; but, this type of components is often characterized by high costs.

Continuous effort has been made to model the capacity-load relationship of CI systems and to enhance the CI performance with limited cost. A homogeneous capacity-load relationship model has been widely used in the study of CIs [8], [9], [12]-[14], [18], whereby the capacity of a link (node) is assumed to be proportional to the initial flow of the link (node) (note that some of the studies focus on link modelling, while others concentrate on modelling node behaviour). However, it has been argued by Kim and Motter that this is unrealistic and empirical data suggests that the relationship between capacity and load of transmission lines is non-linear [17], [19]: heavily loaded lines usually have a lower tolerance parameter than lightly loaded lines. Most recently, Wang and Kim [20] proposed a (non-linear) two-step function for the relationship between the capacity and load of network vertices. Although based on an over-simplified model, it has been shown efficient to prevent cascades by protecting highest-load vertices. Li et al. [21] introduced a more complex heuristic capacity model whereby vertices with both higher loads and larger degrees are

Y.-P. Fang is with the Chair on Systems Science and the Energetic challenge, École Centrale Paris and Supélec, Grande Voie des Vignes, 92290 Châtenay-Malabry, France (e-mail: yiping.fang@ecp.fr)

N. Pedroni is with the Chair on Systems Science and the Energetic challenge, École Centrale Paris and Supélec, Grande Voie des Vignes, 92290 Châtenay-Malabry, France (e-mail: nicola.pedroni@ecp.fr)

E. Zio is with the Chair on Systems Science and the Energetic challenge, École Centrale Paris and Supélec, Grande Voie des Vignes, 92290 Châtenay-Malabry, Paris, France and with Department of Energy, Politecnico di Milano, Milan, Italy (e-mail: enrico.zio@ecp.fr, enrico.zio@supelec.fr, enrico.zio@polimi.it)

paid more extra capacities. It is shown that this model can achieve better network robustness than previous models under the same amount of available resources.

In the present study, we tackle the issue from a systematic perspective by searching for the strategy of resource (capacity) allocation in a power transmission network that is most favourable for resisting to cascading failures, while keeping the total resource (capacity) limited (i.e., while minimizing the network cost). This serves as the primary objective of this paper. In more detail, the problem is formulated within a large-scale, nonlinear and combinatorial multi-objective optimization framework and is solved by a fast and elitist genetic algorithm, namely NSGA-II [22].

The search by the NSGA-II requires also: (i) the construction of a model to describe the cascading failure process in the network of interest, and (ii) the repeated evaluation of the model for every possible capacity allocation pattern proposed by the algorithm during the search. With respect to the model, two approaches are typically considered in the analysis of power transmission systems: complex network theory models, such as the Motter-Lai (ML) model [8], [9] and artificial power flow models, such as the ORNL-Pserc-Alaska (OPA) model [10], [11], [39]. These approaches provide different tradeoffs between the (relatively low) computational cost associated to the model evaluation (allowing applications to large scale power grids) and the (high) level of detail in the system description (including physical characteristics and power flows constraints), respectively.

The OPA model seeks to faithfully describe the dispatching dynamics of the power flows during the evolution of the failure propagation following the initial disturbances, by explicitly incorporating the standard DC power flow equations and minimizing generation cost and load shedding [10]. Embracing this more physical description and solving the constrained linear optimization functions associated to the model, results in a significant increase in the computational burden, rendering practical application extremely difficult for realistic networks with large numbers of elements [23]. For these reasons, topological models based on complex network theory (e.g. the ML model) have emerged in recent years [8], [9], [13], [14], [18], [24]-[26]. In particular, the ML model is a relatively simple and abstract model relying on the resemblance of complex networks to electrical infrastructure systems (in terms of graph theory). It has the advantage of modelling cascading dynamics with few parameters, so that its application to realistic, large-scale networks is feasible and certainly more readily than OPA [16]. However, ML abstracts the power flow laws and constraints of the electrical system. Inevitably, then, it cannot provide direct physical measures of blackout size, but rather abstract measures such as efficiency loss. This has posed questions on whether or not it is adequate in practice, due to its abstract nature, although it has been recognized to offer a new and interesting perspective on the study of cascading failures on power grids [23].

It is worth mentioning that studies tackling the problem of comparison between network-centric approaches and power flow approaches are few in literature. Some studies [23], [25], [27] have provided qualitative comparisons between complex network theory models and power flow models - identifying similarities and differences, and evaluating advantages and disadvantages. Most recently, Correa and Yusta conclude on the appropriateness of graph theory techniques for the assessment of electric network vulnerability by comparison to physical power flow models [28]. By extensive comparative simulation, Cupac et al. have shown that a network-centric model (CLM) exhibits ensemble properties which are consistent with the more realistic OPA fast-scale model [29]. Along these lines, our study takes the comparison a step forward by analyzing the optimization results, enabling to find more interesting insights.

In the present paper, we embrace both the ML and OPA cascading failure models and embed them within NSGA-II for optimally solving the problem of capacity resource allocation. With respect to that, the second objective of the paper is to study the possibility of using a simplified network-centric model (instead of a detailed power flow model) within an optimization framework, without affecting the quality of the optimal solutions found. For illustration, we apply the method to the 400 kV French power transmission network, under the objectives of maximizing network resilience to cascading failures and minimizing investment costs. Finally, we systematically compare the results obtained by using the two cascading failure models of different complexity.

The reminder of this paper is organized as follows. In Section II, we introduce the ML and OPA cascading failure models in detail. We, then, formulate the multi-objective optimization problem taking investment costs and failure resilience into account in Section III. In Section IV, we briefly introduce the procedure of the NSGA-II algorithm. Section V illustrates the French 400kV power transmission network case study and the analysis and comparison of the results. Discussion and conclusion are given in Section VI.

II. Models Of Cascading Failure Considered In This Work

Modelling the dynamic evolution of system-wide cascading failure processes poses a number of challenges due to the diversity of mechanisms which can trigger the initial failure and influence the subsequent propagation of breakdowns in the power system [27]. Various cascading failure models have been proposed; these can be divided into two main categories: those based on complex network theory analysis and those using power flow analysis, often including optimal economic power dispatch after each failure in the propagation, e.g., by linear optimal power flow (OPF) [29].

Complex network theory models, including the ML model adopted in this work and described in Section A below, abstract the representation of a power grid as a graph and then study the connectivity characteristics, the propagation mechanisms through the graph connections and their relationships. These types of models have proved to provide a good understanding of the specific grid dynamics of cascading failures [30]. However, in these models the assumptions only abstract the real loading of the components and the flow distribution

through the connections. For this reason, it is necessary to ascertain the meaningfulness of the results for real electrical infrastructures.

Power flow models, on the contrary, are based on realistic power flow equations to describe the flow dispatching dynamics and failure evolution after the initial disturbances in the power grid. The OPA model, which is the most commonly used of this type of models, is introduced in Section B below and is based on the DC power flow approximation [31].

A. The ML Model

The original ML model has been proposed by Motter and Lai [8], with extensions to differentiate generators and loads [16]. Here, the extended ML model in terms of transmission line failures is utilized. The power transmission network is represented as an undirected graph Q with a set of N vertices representing N_G generators and N_D loads representing distribution substations, interconnected by a set of M edges representing transmission lines. The structure of the network is identified by an $N \times N$ interaction matrix W, whose element w_{ij} is 0 if node i and j are not connected directly; otherwise it is assigned a value of 1, for an unweighted network, or another numerical value, for a weighted network (as in the case of the work in the present paper).

The ML model assumes that at each time step, one unit of the relevant quantity (e.g., electrical flow for power grids) is exchanged between every pair of generator and distributor nodes, and transmitted along the shortest path connecting them. Then, the flow at one link is computed as the number of shortest paths passing through it. More precisely, the flow F_l^{ML} of link l is quantified by the link betweenness, calculated as the fraction of the generator-distributor shortest paths passing through that link:

$$F_l^{ML} = \frac{1}{N_G N_D} \sum_{i \in V_G, j \in V_D} \frac{n_{ij}(l)}{n_{ij}}, l \in E \quad (1)$$

where E ($\|E\| = M$) is the set of all the links in the network; V_G ($\|V_G\| = N_G$) and V_D ($\|V_D\| = N_D$) are the sets of generators and distributors, respectively; n_{ij} is the number of shortest paths between generator nodes and distributor nodes, and $n_{ij}(l)$ is the number of generator-distributor shortest paths passing though link l.

In the *original* ML model [8], a homogeneous capacity-load relationship is assumed: the capacity of link l is assumed to be proportional to its initial flow $F_l^{ML}(0)$ with a network tolerance parameter α:

$$C_l^{ML} = (1 + \alpha) F_l^{ML}(0), l \in E \quad (2)$$

The concept of tolerance parameter α ($\alpha \geq 0$) can be understood as an operating margin allowing safe operation of the component under potential load increment[1]. The occurrence of a cascading failure is initiated by removal of a link, which in general changes the distribution of shortest paths. Then, the flow at a particular link can change and if it increases and exceeds its capacity, the corresponding link fails. Any failure leads to a new redistribution of loads and, as a result, subsequent failures can occur.

Using this cascading failure model, the damage of the network Q can be characterized by the fraction of network efficiency lost in the cascading failure:

$$V_{ML} = \frac{E(Q) - \overline{E(Q)}}{E(Q)} \quad (3)$$

where $V_{ML} \in [0, 1]$ and $\overline{E(Q)}$ represents the residual network structure after the cascading failure. $E(Q)$ measures the network efficiency based on the node pair shortest path distance between generators and distributors. For its computation all pairs of nodes $i \in V_G$, and $j \in V_D$ are weighted by the inverse of their distance:

$$E(Q) = \frac{1}{N_G N_D} \sum_{i \in V_G} \sum_{j \in V_D} \frac{1}{d(i,j)} \quad (4)$$

where $d(i, j)$ is the number of edges for an unweighted network or the sum of edge weights for a weighted network in the shortest path from i to j (like in the present case).

The geodesic network damage V_{ML} measures the functionality of a network when subjected to a contingency due to cascading link disruption with regard to its steady state (base case). As V_{ML} increases, the impact on the network due to cascading failure also increases, as some components become disrupted. V_{ML} has proved to be a well-defined index being capable of providing results consistent with those of physical model indices [28].

The detailed simulation of the ML cascading failure model proceeds as follows:

(1) A random link is chosen as failed and, thus, is removed from the network.

(2) Recur to Eq. (1) and Floyd's shortest paths algorithm to calculate the flow of each working link in the network [32].

(3) Test each link for failure: for each link $l \in E$ of the network, if $F_l^{ML} > C_l^{ML}$ then link l is regarded as failed and, thus, is removed from the network.

(4) If any working link fails, return back to step 2. Otherwise, terminate the simulation and evaluate the network damage by Eq. (3).

Complex network theory models, such as the ML that we use within our optimization framework of the following Section III, have no direct physical relation to the mechanisms of realistic power grids, but they have the key advantage that by utilizing techniques from graph theory they can be applied to analyze large-scale networks. For this reason, this modelling approach is seeing increasing applications for modelling cascading failure processes in power grids.

B. The OPA Model

The OPA model has been proposed by researchers at Oak Ridge National Laboratory (ORNL), Power System Engineering Research Center of Wisconsin University (PSerc), and Alaska University (Alaska) [10], [11]. The OPA model is

[1] In this paper, the link capacities are *variables* to be optimized (see Section III); thus, assumption (2) is obviously not introduced in the problem formulation of the present work.

built upon the Self-Organized Criticality (SOC) theory, contains two different time scale dynamics, i.e., fast power flow dispatching dynamics and slow power grid growth dynamics, and describes the complexity and criticality of power systems. It is a novel and powerful tool for analysing power systems. Our analysis focuses on the fast power flow dynamics, in order to ensure comparability with the ML model shortest path assumption.

The cascading failure model is based on the standard DC power flow equation,

$$F^{OPA} = A \cdot P \tag{5}$$

where F^{OPA} is a vector whose M components are the power flows through the lines, $F_l^{OPA}(l \in E)$, P is a vector whose $N-1$ components are the power injection of each node, P_i (N is the total number of nodes in the network), with the exception of the reference generator, P_0, and A is a constant matrix that depends on the network structure and impedances (see Ref. [10] for details about the computation of A). The reference generator power is not included in the vector P to avoid singularity of A as a consequence of the overall power balance.

The generator power dispatch is solved using standard linear programming methods. Using the input power demand, the power flow Eq. (5) is solved with the condition of minimizing the following cost function:

$$f = \sum_{i \in V_G} P_i(t) + K \sum_{j \in V_D} P_j(t) \tag{6}$$

This definition gives preference to generation shift whilst assigning a high cost (set K =100) to load shedding, and it is assumed that all generators operate at the same cost and that all loads are served with equal priority. The minimization is done with the following constraints:

(5) Generator power injections are generally positive and limited by installed capacity limits: $0 \le P_i \le P_i^{max}, i \in V_G$.

(6) Loads always have negative power injections: $P_j^{dem} \le P_j \le 0, j \in V_D$.

(7) The flow through links is limited by link capacities: $\left|F_l^{OPA}\right| \le C_l^{OPA}$.

(8) Total power generation and consumption remain balanced: $\sum_{i \in V_G \cup V_D} P_i = 0$.

Notice that in order to simplify the power flow problem, making it linear, a number of assumptions have been made in the standard formulation of DC power flow, one of which is that the transmission line resistance is assumed to be negligible i.e. R<<X, i.e. lines are assumed without loss [31]. This means that the loss of power transmission is neglected in the original OPA cascading failure model [10]. However, the objective of cost minimization (Eq. (6)) is only applied to guide the generator power redispatch after the occurrence of a transmission line failure, for which changes in generation or load shedding are usually considered, as the change in transmission loss among different redispatch strategies should probably not be large and considered by the network operator [10].

After solving the linear optimization by using the simplex method as implemented in Flannery et al. [33], we examine which lines are overloaded. A line is considered to be overloaded if the power flow through it is within 1% of the limit capacity C_l^{OPA}. Each overloaded line may outage with probability p_1 (p_1 is set as 1 in the case study to ensure its comparability with ML). If an overloaded line experiences an outage, its power flow limit C_l^{OPA} is divided by a very large number k_1 to ensure that practically no power may flow through the line. Besides, to avoid a matrix singularity from the line outage, the impedances of failed lines are multiplied by a large number k_2, resulting in changes of the network matrix A.

Load shedding is utilized to quantify the damage of the cascading failure. For an individual node, load shedding is defined as the absolute value of the difference between its power injection and demand:

$$LS_j = \left|P_j^{dem} - P_j\right|, j \in V_D \tag{7}$$

Subsequently, total load shedding for the system is:

$$LS = \sum_{j \in V_D} LS_j \tag{8}$$

Finally, system load shedding is normalized by its total demand D and used as a measure of damage to the system resulting from a cascading failure:

$$V_{OPA} = \frac{LS}{D} = \frac{\sum_{j \in V_D} LS_j}{\sum_{j \in V_D} P_j^{dem}} \tag{9}$$

The fact that simulation results from OPA model are consistent with historical blackout data for real power systems has justified its effectiveness [11]. However, the applications of OPA have generally been limited to networks with a relatively small number of nodes compared to real power grids [23], due to the computational efforts involved.

III. Formulation Of The Multi-Objective Optimization Problem

In this section, we generally frame the problem of searching the most favourable pattern of link capacities in a realistic power transmission network, so as to optimize its resilience against cascading failures. By associating a cost to (the capacity of) each link of the network, the optimization process also seeks to minimize the total cost. With the aim of comparing network-centric and power flow approaches, both the ML and OPA models introduced in Section II are used to evaluate the vulnerability of the pattern of link capacities proposed during the optimization search.

Specifically, we define the variables to be optimized as the capacities of the links in the network, $C_l, l \in E$ (i.e., C_l^{ML} for the ML model and C_l^{OPA} for the OPA model). Thus, the homogeneous capacity allocation strategy as expressed in Eq. (2) is no longer adopted in the optimization. Instead, any non-negative vector $C \in \boldsymbol{R}_+^M$ could represent a potential solution. It is noted that the searching space $\boldsymbol{R}_+^M$ is intractably large in reality, where a power transmission network usually has hundreds or thousands of links.

We, then, assume that the cost associated with each link capacity is linearly proportional to the value of the capacity, with coefficient φ (we simply set φ as 1 in our case study). The total investment cost related to a capacity allocation pattern $C \in \boldsymbol{R}_+^M$ in the power transmission network can, then, be defined as:

$$Cost(C) = \sum_{l \in E} \varphi C_l \quad (10)$$

The network damage resulting from a cascading failure in the presence of a given capacity pattern can be obtained by running the ML (or the OPA) simulation in correspondence of the capacity pattern and, then, using Eq. (3) (or Eq. (9) for OPA). The cascade is initiated by the failure of a single link in each model. The single link is randomly selected from the set of links E in the network with equal probability. Then, the algorithms for cascading simulation proposed in Section II are applied. The cascade simulations run over several iterations until they either converge or exceed the maximum number of steps (we use maximum 20 iterations for both ML and OPA). Finally, the network vulnerability for a given capacity allocation pattern C is obtained as the average network damage $\overline{V_{ML}}$ (or $\overline{V_{OPA}}$ for OPA), over various random triggers (we use 30 triggers for both ML and OPA).

Through the quantification of the capacity allocation cost and cascading failure vulnerability, the capacity allocation problem is formulated as a multi-objective optimization:

$$\begin{cases} \min\limits_{C \in \boldsymbol{R}_+^M} Cost(C) & (11) \\ \min\limits_{C \in \boldsymbol{R}_+^M} \overline{V}(C) & (12) \end{cases}$$

The objective function (11) is the sum of the link capacity costs; function (12) expresses the cascade vulnerability objective, where $\overline{V}(C)$ is $\overline{V_{ML}}$ when the ML model is used, or $\overline{V_{OPA}}$ when OPA is used. Observe that under this definition the most cascade-resilient network might be the network with infinite capacity, which obviously would conflict with the objective of minimizing cost.

IV. Multi-Objective Evolutionary Algorithms (MOEA) For Optimal Capacity Allocation

Multi-objective evolutionary algorithms (MOEAs) have proven to be general, robust and powerful search tools that are desirable for tackling problems involving i) multiple conflicting objectives, and ii) intractably large and highly complex search spaces [34]. In extreme synthesis, the main properties of Evolutionary Algorithms (EAs) are that the search for the optima is conducted (i) using a (possibly) large population of multiple solution points or candidates, (ii) using operations inspired by the evolution of species, such as breeding and genetic mutation, (iii) using probabilistic operations and (iv) using information on the objective or search functions and not on its derivatives. The main advantages are: (i) fast convergence to near global optima, (ii) superior global searching capability in complicated search spaces and (iii) applicability even when gradient information is not readily achievable. MOEAs rely on the following concepts [35]:

- Pareto front: The locus that is formed by a set of solutions that are equally good when compared to other solutions of that set is called Pareto front.
- Non-Domination: Non-dominated or Pareto-optimal solutions are those solutions in the set which do not dominate each other, i.e., neither of them is better than the other in all the objective function evaluations. The solutions on each Pareto front are Pareto-optimal with respect to each other.

In this study, we use a fast and elitist genetic algorithm, namely, NSGA-II [22], to solve the multi-objective optimization problem (11)-(12). NSGA-II has been proved to be an efficient algorithm to find Pareto optimal solutions [36]; for further details about this algorithm and relevant surveys on multi-objective evolutionary optimization, the reader is referred to Ref. [22], [34]-[36]. The complete procedure for our capacity allocation optimization problem is detailed as follows:

(1) Read power transmission network data (line, bus, adjacency matrix, etc.) and fix the MOEA parameters (i.e., population size, maximum generation, etc.);

(2) Randomly initialize a (parent) population of possible solutions (individuals) and evaluate the fitness of each individual with respect to the two objective functions (11) and (12); sort the parent population according to the non-domination criterion [35];

(3) Select the parents which are fitter for reproduction by using a binary tournament selection [22]; the procedure is such that fitter individuals are selected with a higher probability;

(4) Generate an offspring population by crossover and mutation operators, and evaluate the fitness of each individual in the offspring population with respect to the two objective functions (11) and (12);

(5) Combine the parent and offspring populations to generate a new "trial" aggregate population and perform non-dominated sorting on the "trial" population;

(6) Generate a new parent population by selecting the best solutions in the sorted "trial" population, until a desired population size is reached;

(7) If the stop condition is met, then terminate the iteration; otherwise, go to step 3.

The non-dominated solutions of the last population constitute the Pareto optimal front of the optimization problem at hand.

V. Case Study And Results Analysis

A. Case Study and Parameters Setting

In this paper, the 400kV French power transmission network (FPTN400) (Fig. 1) is taken for exemplification of the proposed approach. The network is built from the data on the 400 kV transmission lines of the RTE website [37]. It has 171 nodes (substations) and 220 edges (transmission lines). We distinguish the generators, which are the source of power, from the other distribution substations, that receive power and transmit it to other substations or distribute it in local distribution grids. By obtaining the power plants list from EDF website [38] and relating them with the ID of the buses in the transmission network, we have 26 generators and 145 distributors. Only the nuclear power plants, hydroelectric plants and thermal power plants whose installed capacities are larger than 1000 MW, are considered. Although simplifications have been made, the network model still has sufficient details to illustrate the validity of the method on a realistic-size electrical infrastructure.

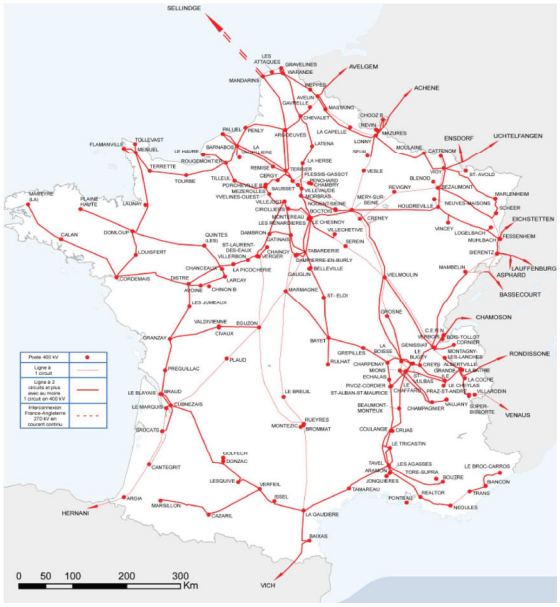


Fig. 1. The 400kV French power transmission network (FPTN400) [37].

For optimal allocation of link capacity in the network, the NSGA-II algorithm introduced in Section IV is applied with regards to the objectives of minimizing cascade vulnerability and investment cost, expressed by functions (11) and (12) respectively. Both the ML and OPA models are used to evaluate the cascade vulnerability of the proposed network. The parameters values used in the NSGA-II algorithm are reported in Table I. In this study, we do not attempt to find the best optimal setting for each of the NSGA-II parameters and they have been set by trial and error guided by the aim of reaching convergence. For the interested reader, extensive studies exist especially focusing on the task of tuning GA parameters [40], [41], [42].

TABLE I
Parameters Of The NSGA-II Algorithm

Parameters	Values
Population size	80
Maximum generation	1500
Crossover probability	0.9
Mutation probability	0.1
Crossover operator	20
Mutation operator	20

B. Comparison between the ML and OPA Models

1) Model Adjustments and Settings

The comparison between the optimization results of the ML and OPA models is not straightforward due to the differences of the two models in the way of representing system flow, in the iterative algorithms they rely on, and in the way of measuring the damage produced by the cascading failure. Accordingly, some assumptions and adjustments to the models are necessary to ensure their comparability.

Flow initialization: In the ML model, initial link flow is calculated directly by Eq. (1). Regarding the OPA model, the calculation of initial link power flow by Eq. (5) necessitates data about power demand and generator capacity. Prior studies set this data by evolving the network using combined fast-slow dynamics until the network reaches a steady state [10], [11]. In order to ensure comparability with ML, and taking into account that we limit the scope of our comparison to fast dynamics, we use a simpler initialization strategy that does not require the consideration of network upgrades over time.

Although the ML model does not represent demand and generation capacity quantitatively, it assumes that every distributor is connected to every generator, whereby there is only one shortest path from any distributor to every generator. This implies that every distributor attempts to extract an equal amount of power from every generator [29]. Thus, to facilitate comparability with the ML model, we use the following assumptions in OPA: (i) all the loads have equal constant power demand, and (ii) the total generation capacity is set to be equal to the total demand and equally divided among the generators.

In Fig. 2, we plot the relationship between the initial flow of each link determined using the ML model and that determined using the OPA model in the FPTN400. Each green square in the Figure corresponds to one of the links in the network. The x-axis is the value of initial flow of the link in ML, and its y-axis is the value of its initial flow in the OPA approach. It can be seen that the initial link flow in ML is highly correlated with the initial link flow in OPA, computed by means of the proposed initialization method (the correlation coefficient $r_{ML,OPA}$ is equal to 0.77). That is to say, links with high initial flow in ML tend to have high initial flow in OPA, and vice versa. This shows that our initialization strategy is consistent for ML and OPA.

Cost normalization: Since the ML and OPA models rely on different variables and algorithms (see Section II), the numerical values of each link flow and capacity determined within the two approaches are obviously not identical. Therefore, in order to facilitate the comparison of the

optimization results from the two approaches, the cost of each capacity (allocation pattern) proposed by the optimization algorithm is normalized by the corresponding total initial network flow[2], and indicated as $\overline{Cost}$ in both the ML and OPA models.

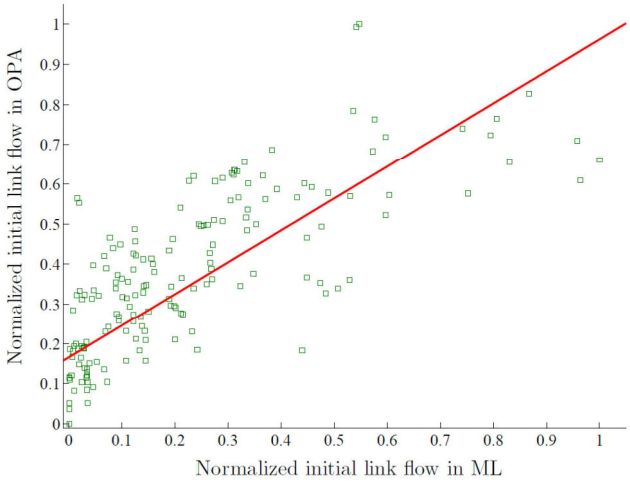


Fig. 2. Scatter-plot of the normalized initial link flows in the ML and OPA models, with reference to the 400kV French power transmission network. The initial link flow in ML is highly correlated to that in OPA ($r_{ML,OPA}$=0.77). The best fit line is also shown.

Comparison method: As already mentioned before, it is evident that the ML and OPA models provide different results at the local scale [29]; however, we evaluate to what extent the two approaches are consistent at the global system level. In particular, we compare the two approaches by performing the following analyses:

- We verify whether the Pareto fronts based on the ML and OPA models exhibit similar characteristics in terms of phase transitions of cascade vulnerability with respect to normalized investment cost;
- We investigate whether the Pareto optimal solutions showing the same level of investment cost also present similar capacity allocation patterns;
- We examine whether the link capacities patterns along the two optimal frontiers exhibit similar characteristics for decreasing network vulnerability (i.e. for increasing network resilience).

2) Comparison Results

We first investigate the shape of the Pareto fronts obtained using the ML and OPA models in the capacity allocation optimization: in particular, we analyze the variation of cascade vulnerability as a function of normalized investment cost. Notice that a proper comparison of the Pareto fronts obtained with the ML and OPA models is only possible with the adjustments proposed in previous Section. Fig. 3 shows that ML and OPA Pareto fronts exhibit similar phase transitions (although their absolute values are different, which is not unexpected considering the fact that they apply different modelling parameters and cascade vulnerability measures): both curves present a sharp decrease in network vulnerability in the same $\overline{Cost}$ region (i.e. $1.0 \leq \overline{Cost} \leq 1.5$), where a small increase in the cost gives a large gain in terms of cascade resilience. Besides, regions of plateau exist for certain cost values in both models (i.e. for $1.5 \leq \overline{Cost} \leq 1.75$ and $2.0 \leq \overline{Cost} \leq 2.2$ in ML, and for $1.5 \leq \overline{Cost} \leq 1.8$ and $2.15 \leq \overline{Cost} \leq 2.45$ in OPA), in which increasing investment cost does not improve network resilience. Finally, both curves show a relatively stable regime for large $\overline{Cost}$ values (i.e., $\overline{Cost} \geq 2.2$), where network resilience is already high and its relative improvement is negligible even for a significant increase in the network cost (for example, referring to the ML model, increasing $\overline{Cost}$ from 1.97 to 2.61, i.e., of 32.5%, we reduce the network vulnerability of only 1.5%). One could refer to the Pareto fronts of ML (squares in left panel) and OPA (triangles in right panel) in Fig. 4, where this relative stable regime is shown more clearly on a linear y-axis scale.

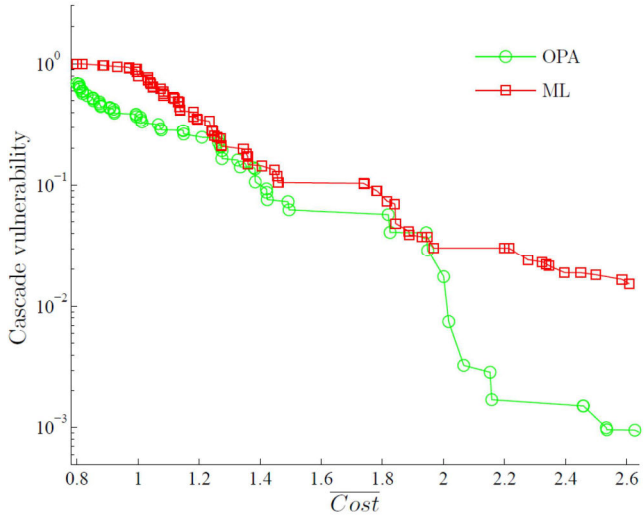


Fig. 3. Phase transitions in the Pareto optimal fronts showing cascade vulnerability (i.e., average efficiency loss for ML and average load shedding for OPA) with respect to normalized investment cost.

In Fig. 4 we compare the Pareto fronts obtained by the ML and OPA models within the multi-objective optimization framework of Section III with the results obtained by assuming a classical homogeneous capacity allocation strategy (see Section II.A). The capacity in the homogeneous capacity allocation is assumed to be linearly proportional to the initial flow by means of the network tolerance parameter α, as indicated in Eq. (2); thus, the normalized cost of a given capacity allocation pattern is precisely equal to parameter α by construction. It can be seen that in both cases the multi-objective optimization approach based on ML and OPA produces superior solutions as the corresponding Pareto fronts are closer to the coordinate axes. The linear (homogeneous) capacity-load relationship evidently appears not optimal for obtaining a cost-efficient and cascade-resilient network.

We, then, compare the link capacities patterns of those solutions along the two Pareto fronts that present

[2] By this definition, the normalized cost has precisely the same physical meaning with the network tolerance parameter α.

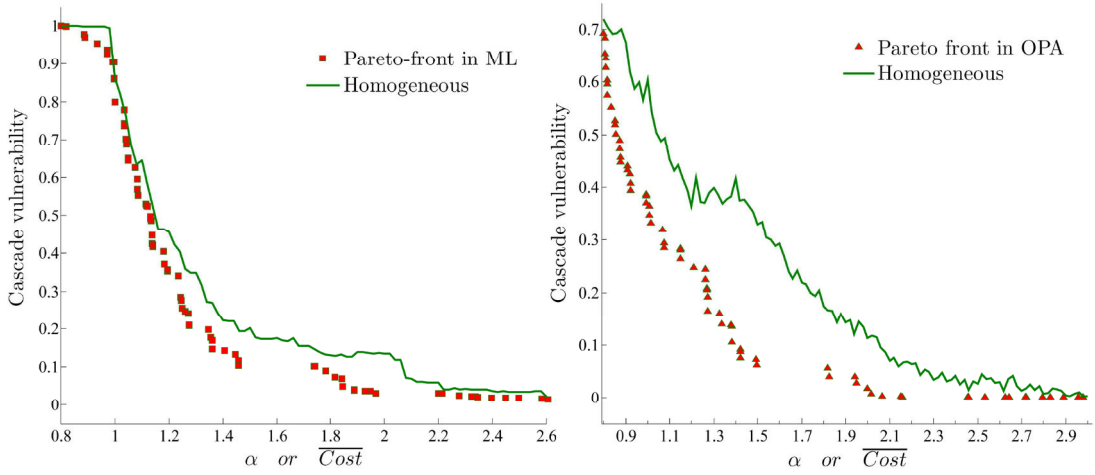


Fig. 4. ML (left panel) and OPA (right panel) Pareto fronts obtained in the multi-objective optimization framework of Section III (squares and triangles), together with the results obtained by employing a homogeneous capacity allocation strategy (solid line).

approximately the same values of $\overline{Cost}$. In particular, three representative values of normalized cost (i.e., $\overline{Cost}$=1.07, 1.27 and 1.81) along the Pareto fronts are chosen, and the relationship between the link capacities of the corresponding optimal solutions obtained by the ML and OPA models are visualized using the scatterplots of Fig. 5(a), (b) and (c), respectively. It is evident that the link capacities of the optimal solutions based on the ML and OPA models are highly correlated (with correlation coefficient $r_{ML,OPA}$=0.73, 0.69 and 0.76, respectively). That is, links with low capacity in the ML model are likely to have low capacity also in the OPA model, and links with high capacity in ML also have high capacity in OPA.

Finally, it is interesting to analyse how the pattern of link capacities changes when lower network cascade vulnerability (higher network resilience) is demanded, i.e., which type of capacity allocation pattern is the most favourable in resisting to cascading failure. We tackle this problem by investigating the "expected" network link capacity pattern as a function of cascade vulnerability, i.e., the configuration of capacity pattern "averaged" over all possible solutions of the Pareto front lying within a given "regime" (i.e., interval) of cascade vulnerability of interest. Parameter β^s (namely, β^s_{ML} for ML and β^s_{OPA} for OPA) is used to represent the "regime" of vulnerability, where s indicates the size of the corresponding interval. It is noted that smaller β^s represents higher network resilience.

Fig. 6 reports the results of averaged link capacities patterns for three different levels of cascade vulnerability, i.e., $0.6 \le \beta^{0.1} \le 0.7$, $0.3 \le \beta^{0.1} \le 0.4$ and $0 \le \beta^{0.1} \le 0.1$ in the case of a homogeneous allocation strategy (circles) and of the optimization-based approach in our study (squares). The left panel (a-c) is referred to ML, whereas the right panel (d-f) relates to OPA. It is found that the optimal link capacity patterns exhibit consistent characteristics between ML and OPA models. For example, in both cases, the optimal link capacities patterns are similar to their corresponding homogeneous allocations only in less resilient networks, i.e., when $0.6 \le \beta^{0.1} \le 0.7$, where the objective of minimizing investment cost is much more biased (Fig. 6(a) and (d)). When we increase the importance of minimizing the network vulnerability (e.g., for $0.3 \le \beta^{0.1} \le 0.4$ and $0 \le \beta^{0.1} \le 0.1$), the optimal link capacities show a non-linear relationship with respect to their initial flows, as shown in Fig. 6(b), (c) and Fig. 6(e), (f). Specifically, the heavily loaded links tend to decrease their capacities and the lightly loaded links tend to increase their capacities. That is to say, the unoccupied portion of capacity tends to decrease in links with larger loads and the unoccupied portion of capacity tends to increase in the less loaded links. Furthermore, the more importance is given to the minimization of network cascade vulnerability, the more pronounced the non-linear behaviour is, as shown in Fig. 6(c) and (f). Our findings are consistent with the empirical observations and results from the traffic fluctuation model [17], [19].

VI. Discussion And Conclusion

In this paper, we have tackled the problem of searching for the most favourable pattern of link capacity allocation for a CI network with the objective of resisting to cascading failures with limited investment costs. The problem has been formulated within a multi-objective optimization framework and has been solved by an evolutionary algorithm, namely the NSGA-II. The optimization has been carried out using two different approaches to cascade failure modelling: a computationally-cheap complex network model -- namely, the Motter-Lai (ML) model -- and a more detailed power flow model -- namely, the ORNL-Pserc-Alaska (OPA) model. The approaches have been compared on a case study involving the 400kV French power transmission network (FPTN400). Although simplifications have been applied, the network model still has sufficient detail to illustrate the validity of the method on a realistic electrical infrastructure.

The objective of this paper is twofold: 1) to tackle the issue of capacity-load relationship from a systematic perspective, by

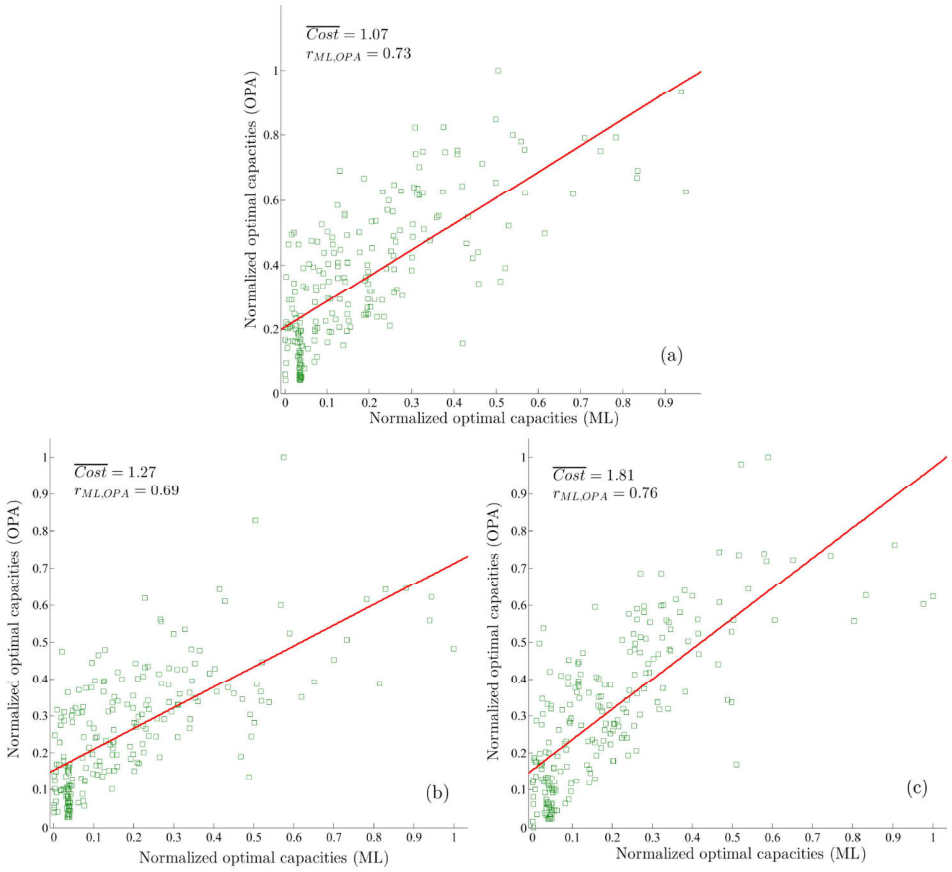


Fig. 5. Scatter plot of the (normalized) link capacities of three representative ML and OPA Pareto solutions showing the same normalized cost. The link capacities of the Pareto solutions with the same level of cost show highly correlated allocation patterns: (a) ML solution (1.07, 0.63) versus OPA solution (1.07, 0.30): $r_{ML,OPA} = 0.73$; (b) ML solution (1.27, 0.24) versus OPA solution (1.27, 0.21): $r_{ML,OPA} = 0.69$; (c) ML solution (1.81, 0.074) versus OPA solution (1.81, 0.057): $r_{ML,OPA} = 0.76$. The line of best fit is also plotted, for visual guidance.

introducing the optimization of link capacity allocation, and 2) to study the possibility of using a simplified network-centric model (instead of a detailed power flow model) within the optimization framework, without affecting the quality of the optimal solutions found, by embedding both the ML and OPA model into the optimization and comparing their results.

Primarily, our multi-objective optimization results show that both the ML and OPA models produce improved Pareto solutions with respect to those obtained by assuming a classical homogeneous allocation strategy. In addition, the optimal link capacity allocations show a non-linear capacity-load relation: the unoccupied portion of capacity tends to decrease in links with larger loads, whereas the unoccupied portion of capacity tends to increase in the lightly loaded links. This is in sharp contrast with the linear capacity-load relation hypothesized in previous works of literature [8], [9], [12]-[14], [18]. This non-linear behaviour is probably a consequence of the following observation: since larger loads in heavily loaded components tend to result from a large number of flow events, the relative size of the fluctuations in these components tends to be small when other lightly loaded components fail during a cascading failure; considering that the unoccupied capacity is the operating margin that allow safe operation for the component under potential load increment (mainly determined by the perturbations caused by the failure of other components of the network), this explains why in the optimal solutions the unoccupied capacity tends to be smaller for links with larger loads.

Additionally, the analysis of the behaviour of the link capacity patterns of the Pareto optimal solutions as a function of the vulnerability level has shown that the results provided by ML and OPA are consistent: the more importance is given to the objective of network cascade vulnerability, the more pronounced is the non-linear capacity-load relation for both models. Besides, the Pareto fronts produced by ML and OPA exhibit similar phase transitions. Both curves exhibit a sharp decrease in network vulnerability when $1.0 \leq \overline{Cost} \leq 1.5$, a plateau for certain cost values (i.e., for $1.5 \leq \overline{Cost} \leq 1.75$ and $2.0 \leq \overline{Cost} \leq 2.2$ in ML, and for $1.5 \leq \overline{Cost} \leq 1.8$ and $2.15 \leq \overline{Cost} \leq 2.45$ in OPA) and a relatively stable regime when $\overline{Cost} \geq 2.2$. Furthermore, the link capacities of the Pareto optimal solutions produced by the ML and OPA models show highly correlated allocation pattern, which means that links with low capacity in ML tend to have low capacity in OPA, and links with high capacity in ML also tend to have high

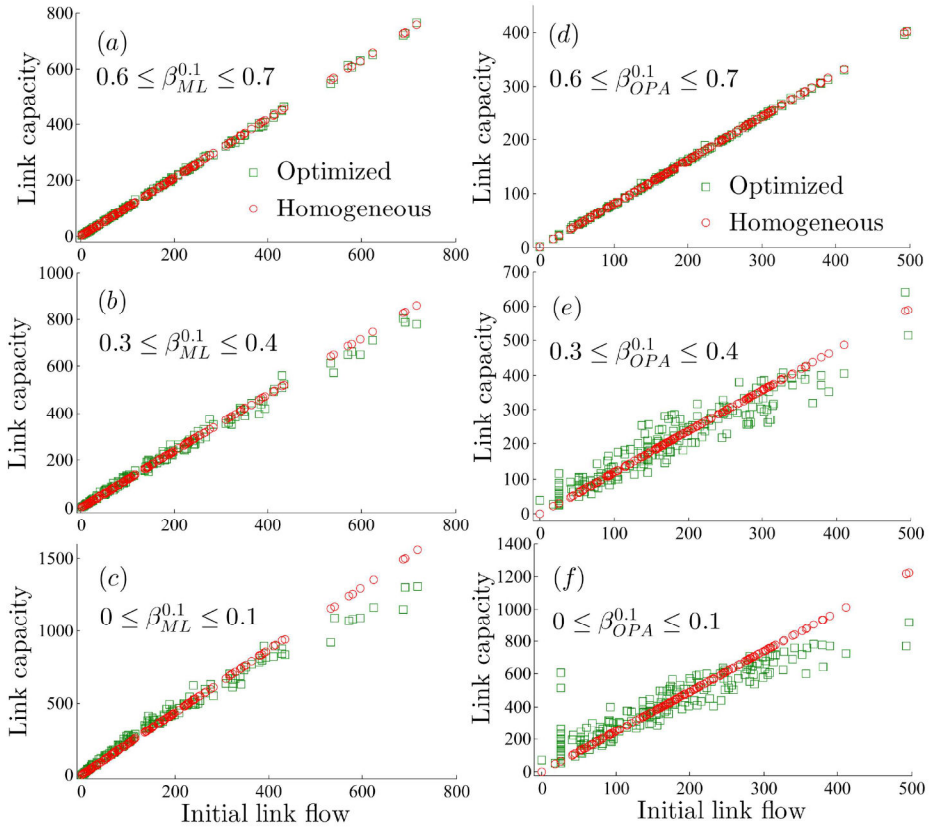


Fig. 6. "Averaged" optimal link capacity patterns for three different levels of cascade vulnerability ($0.6 \leq \beta^{0.1} \leq 0.7$, $0.3 \leq \beta^{0.1} \leq 0.4$ and $0 \leq \beta^{0.1} \leq 0.1$) in ML (left panel a-c) and OPA (right panel d-f). The scatter plot shows the relationship between the link capacities and the initial link flows in a homogeneous allocation strategy, where the capacity of a link is assumed to be proportional to its initial flow (circles) and after in the optimization-based approach of Section III (squares).

capacity in OPA. This consistency is not insignificant since it demonstrates that one resilience-improved pattern of capacity allocation optimized by the ML model is also of higher resilience if measured by the more realistic OPA model.

The results from this comparative study provide an important contribution regarding the usefulness of a topological model (ML) in the optimization of a cascade resilient electrical network. Although ML is a relatively simple and abstract model (that does not account for the power flow laws and constraints of the electrical system), it is able to provide results that are consistent with a detailed and more realistic power flow model (OPA), when applied to the problem of network optimization against cascading failure. Most importantly, with respect to OPA it has the advantages of simplicity and scalability: the average time needed to carry out a single cascade failure simulation is 3.9s and 20.8s for ML and OPA, respectively, on a double 2.4 GHz Intel CPU and 4 GB RAM computer. This provides impetus for the use of network-centric models to the study of cascading failure in large power network systems.

Future works may consider comparing our optimization results with real data, i.e. the empirical capacity-load characteristics, for extracting further insights about how realistic infrastructure systems evolve. Besides, it is noted that the optimization based on the OPA model leads to solutions of reduced vulnerability compared to its ML counterpart (see Fig. 4) and the modelling reason behind it, is worthy of further study. Furthermore, Newton Raphson-based power flow approaches [43] could be applied for the comparison with the ML model, since they give a more detailed depiction of the cascading failure process, although the price to be paid is that they are computationally expensive. Finally, it would be interesting to apply our method to other networks, e.g. the standard IEEE Power Systems Test Cases and the like.

REFERENCES

[1] U.-C. P. S. O. T. Force, "Final report on the august 14, 2003 blackout in the United States and Canada: causes and recommendations," U.S.-Canada Power System Outage Task Force, Tech. Rep., 2004.

[2] U. for the Coordination of Transmission of Electricity, "Final report system disturbance on 4 nov. 2006," Union for the Coordination of Transmission of Electricity, Tech. Rep., 2007.

[3] J. J. Romero, "Blackouts illuminate India's power problems," *Spectrum, IEEE*, vol. 49, no. 10, pp. 11–12, 2012.

[4] S. Battiston, D. Delli Gatti, M. Gallegati, B. Greenwald, and J. E. Stiglitz, "Credit chains and bankruptcy propagation in production networks," *Journal of Economic Dynamics and Control*, vol. 31, no. 6, pp. 2061–2084, 2007.

[5] M. E. Newman, S. Forrest, and J. Balthrop, "Email networks and the spread of computer viruses," *Physical Review E*, vol. 66, no. 3, p. 035101, 2002.

[6] K. Zhao, A. Kumar, T. P. Harrison, and J. Yen, "Analyzing the resilience of complex supply network topologies against random and targeted disruptions," *Systems Journal, IEEE*, vol. 5, no. 1, pp. 28–39, 2011.

[7] D. Kempe, J. Kleinberg, and ´ E. Tardos, "Maximizing the spread of influence through a social network," in *Proceedings of the 9th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2003, pp. 137–146.

[8] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, p. 065102, 2002.

[9] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, no. 4, p. 045104, 2004.

[10] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "An initial model for complex dynamics in electric power system blackouts," in *Proceedings of Annual Hawaii International Conference on System Sciences*, 2001, pp. 51–51.

[11] B. A. Carreras, D. E. Newman, I. Dobson, and A. B. Poole, "Evidence for self-organized criticality in a time series of electric power system blackouts," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 51, no. 9, pp. 1733–1740, 2004.

[12] A. E. Motter, "Cascade control and defense in complex networks," Physical Review Letters, vol. 93, no. 9, p. 098701, 2004.

[13] Y. Li, G. Sansavini, and E. Zio, "Non-dominated sorting binary differential evolution for the multi-objective optimization of cascading failures protection in complex networks," *Reliability Engineering & System Safety*, vol. 111, no. 0, pp. 195 – 205, 2013.

[14] Y.-P. Fang, E. Zio et al., "Optimal production facility allocation for failure resilient critical infrastructures," in *Proceedings of the 22nd European Safety and Reliability (ESREL 2013) annual conference*, Sep. 2013, pp. 2605–2612.

[15] L. Zhao, K. Park, and Y.-C. Lai, "Attack vulnerability of scale-free networks due to cascading breakdown," *Physical review E*, vol. 70, no. 3, p. 035101, 2004.

[16] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north American power grid," *The European Physical Journal B - Condensed Matter and Complex Systems*, vol. 46, no. 1, pp. 101–107, 2005.

[17] D.-H. Kim and A. E. Motter, "Fluctuation-driven capacity distribution in complex networks," *New Journal of Physics*, vol. 10, no. 5, p. 053022, 2008.

[18] E. Zio and G. Sansavini, "Modeling interdependent network systems for identifying cascade-safe operating margins," *Reliability, IEEE Transactions on*, vol. 60, no. 1, pp. 94–101, 2011.

[19] D.-H. Kim and A. E. Motter, "Resource allocation pattern in infrastructure networks," *Journal of physics A: mathematical and theoretical*, vol. 41, no. 22, p. 224019, 2008.

[20] B. Wang and B. J. Kim, "A high-robustness and low-cost model for cascading failures," *EPL (Europhysics Letters)*, vol. 78, no. 4, p. 48001, 2007.

[21] P. Li, B.-H. Wang, H. Sun, P. Gao, and T. Zhou, "A limited resource model of fault-tolerant capability against cascading failure of complex network," *The European Physical Journal B*, vol. 62, no. 1, pp. 101–104, 2008.

[22] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: Nsga-ii," *Evolutionary Computation, IEEE Transactions on*, vol. 6, no. 2, pp. 182–197, 2002.

[23] K. Sun and Z.-X. Han, "Analysis and comparison on several kinds of models of cascading failure in power system," in *Transmission and Distribution Conference and Exhibition: Asia and Pacific*, 2005 IEEE/PES. IEEE, 2005, pp. 1–7.

[24] B. Y. Calida, A. V. Gheorghe, R. Unal, and D. Vamanu, "Dealing with next generation infrastructures academic programmes complexity induced resiliency assessment," *International Journal of Critical Infrastructures*, vol. 6, no. 4, pp. 347–362, 2010.

[25] S. LaRocca, J. Johansson, H. Hassel, and S. Guikema, "Topological performance measures as surrogates for physical flow models for risk and vulnerability analysis for electric power systems," *arXiv preprint*, arXiv:1306.6696, 2013.

[26] P. Zhang, B. Cheng, Z. Zhao, D. Li, G. Lu, Y. Wang, and J. Xiao, "The robustness of interdependent transportation networks under targeted attack," *EPL (Europhysics Letters)*, vol. 103, no. 6, p. 68005, 2013.

[27] R. Baldick, B. Chowdhury, I. Dobson, Z. Dong, B. Gou, D. Hawkins, H. Huang, M. Joung, D. Kirschen, F. Li et al., "Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures," in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, 2008 IEEE. IEEE, 2008, pp. 1–8.

[28] G. J. Correa and J. M. Yusta, "Grid vulnerability analysis based on scale-free graphs versus power flow models," *Electric Power Systems Research*, vol. 101, pp. 71–79, 2013.

[29] V. Cupac, J. T. Lizier, and M. Prokopenko, "Comparing dynamics of cascading failures between network-centric and power flow models," *International Journal of Electrical Power & Energy Systems*, vol. 49, pp. 369–379, 2013.

[30] A°. J. Holmgren, "Using graph models to analyze the vulnerability of electric power networks," *Risk analysis*, vol. 26, no. 4, pp. 955–969, 2006.

[31] K. Purchala, L. Meeus, D. Van Dommelen, and R. Belmans, "Usefulness of dc power flow for active power flow analysis," *in Power Engineering Society General Meeting*, 2005. IEEE. IEEE, 2005, pp. 454–459.

[32] R. W. Floyd, "Algorithm 97: Shortest path," *Commun. ACM*, vol. 5, no. 6, pp. 345–, Jun. 1962.

[33] B. P. Flannery, W. H. Press, S. A. Teukolsky, and W. Vetterling, *Numerical recipes in c*, Press Syndicate of the University of Cambridge, New York, 1992.

[34] E. Zitzler, M. Laumanns, and S. Bleuler, "A tutorial on evolutionary multiobjective optimization," in *Metaheuristics for Multiobjective Optimisation*. Springer, 2004, pp. 3–37.

[35] K. Deb, Multi-objective optimization using evolutionary algorithms, vol. 2012. Chichester: John Wiley & Sons, 2001.

[36] A. Konak, D. W. Coit, and A. E. Smith, "Multi-objective optimization using genetic algorithms: A tutorial," *Reliability Engineering & System Safety*, vol. 91, no. 9, pp. 992–1007, 2006.

[37] RTE, "Le réseau de transport d'électricité 400kv," www.rte-france.com/uploads/media/CS4_2013.pdf, November 2013.

[38] EDF, "En direct de nos centrales," http://france.edf.com/france-45634.html/, Avril 2013.

[39] S. Mei, F. He, X. Zhang, S. Wu, and G. Wang, "An improved OPA model and blackout risk assessment," *Power Systems, IEEE Transactions on*, 24(2), 814-823, 2009.

[40] A. E. Eiben, Z. Michalewicz, M. Schoenauer, and J. E. Smith, "Parameter control in evolutionary algorithms," In *Parameter setting in evolutionary algorithms*, pp. 19-46, Springer Berlin Heidelberg, 2007.

[41] K. De Jong, "Parameter setting in EAs: a 30 year perspective," In *Parameter Setting in Evolutionary Algorithms*, pp. 1-18. Springer Berlin Heidelberg, 2007.

[42] M. E. Samples, M. J. Byom, and J. M. Daida, "Parameter sweeps for exploring parameter spaces of genetic and evolutionary algorithms," In *Parameter Setting in Evolutionary Algorithms*, pp. 161-184, Springer Berlin Heidelberg, 2007.

[43] H. Wang, and J. S. Thorp, "Optimal locations for protection system enhancement: a simulation of cascading outages," *Power Delivery, IEEE Transactions on*, 16(4), pp. 528-533, 2001.

Paper [5] Y.-P. Fang, N. Pedroni, E. Zio. "Assessment and optimization of system resilience for infrastructure network systems." IEEE System Journal, 2014, under review.

Assessment and Optimization of the Resilience of Infrastructure Network Systems Subject to Disruptive Events

Y.-P. Fang, N. Pedroni, and E. Zio, *Senior Member, IEEE*

***Abstract*—This study firstly proposes a new quantitative metric of system resilience, which focuses on the post-disaster recovery process describing how the system "bounces back" from a distress to a normal functioning state. Based on this metric, we formulate a bi-level resilience optimization model for selecting proper recovery actions in order to enhance the resilience of infrastructure networks. The resilience optimization problem (ROP) is formulated within a mixed integer programming (MIP) framework, and a heuristic dispatching rule that integrates concepts from network flows and project scheduling is proposed for its solution. A case study involving the 400kV French Power Transmission Network (FPTN400) shows that the proposed method is able to produce high-quality sub-optimal solutions to the ROP with much less computational cost than the MIP approach based on a branch and cut algorithm. This looks promising for the use of the proposed heuristic dispatching rule in restoration activities on large-scale infrastructure networks.**

***Index Terms*— Infrastructure networks, system resilience, system recovery, dispatching rules, optimization**

I. Introduction

Critical infrastructures (CIs) are network systems designed and operated to deliver resources and services to consumers and businesses in an efficient manner. Examples of such CIs are power grids, telecommunication networks, transportation networks, etc. Disruptive events, whether they are malevolent attacks, natural disasters, or human-caused accidents, can have significant direct and indirect impacts.

Justifiably, then, critical infrastructure protection (CIP) has gained great importance in all nations, with particular focus being placed traditionally on physical protection and asset hardening [1]-[4]. In recent years, lessons learned from some catastrophic accidents have pushed part of the focus on the concept of "resilience" – i.e., the ability of an infrastructure system to withstand, adapt to, and rapidly recover from the effects of a disruptive event [6], [7]. The outcomes of the 2005 World Conference on Disaster Reduction (WCDR) confirmed the significance of the entrance of the term resilience into disaster discourse and gave birth to a new culture of disaster response [9]. As a result, systems should not only be reliable, i.e. having an acceptably low failure probability, but also resilient, i.e. having the ability to recover from disruptions [8]. Government policy has also evolved to encourage efforts that would allow assets to continue operating at some level, or quickly return to full operation after the occurrence of disruptive event [5].

Resilience comes from the Latin word "resilio" that literary means "to leap back" and denotes a system attribute characterized by the ability to recover from challenges or disruptive events. The Merriam-Webster dictionary defines resilience as "the ability to recover from or adjust easily to misfortune or change." Various definitions of "resilience" have been proposed for infrastructure and economic system analysis in the past decades, e.g., see [9]-[16], [29]. Unfortunately there is currently a lack of standardization and rigor when quantitatively defining resilience [15]. Too many different and subjective definitions (some of them overlap significantly with a number of already existing concepts like robustness, vulnerability and survivability) make resilience appear to be just another buzzword and not an attribute of engineering systems. To address this issue, this study firstly reviews different resilience metrics and measurement methodologies in the context of systems engineering especially for CI systems; then, it proposes a novel quantification of system resilience focusing on the post-disaster recovery process, which describes how the system "bounces back" from a distress to a normal state.

While resilience can be characterized by many system features and attributes, recovery is a vital element of strategies to improve resilience. System recovery and its role in infrastructure network resilience have attracted much previous attention. Some studies have modelled the post-disaster restoration of various infrastructure systems in an effort to estimate the expected restoration time [17]-[19], and several others have compared the performance of different restoration strategies [20], [21]. More works have been done to tackle the problem of post-disaster restoration strategy planning and optimization for the purpose of restoring system service in a

Y.-P. Fang is with the Chair on Systems Science and the Energetic challenge, École Centrale Paris and Supélec, Grande Voie des Vignes, 92290 Châtenay-Malabry, France (e-mail: yiping.fang@ecp.fr)

N. Pedroni is with the Chair on Systems Science and the Energetic challenge, École Centrale Paris and Supélec, Grande Voie des Vignes, 92290 Châtenay-Malabry, France (e-mail: nicola.pedroni@ecp.fr)

E. Zio is with the Chair on Systems Science and the Energetic challenge, École Centrale Paris and Supélec, Grande Voie des Vignes, 92290 Châtenay-Malabry, Paris, France and with Department of Energy, Politecnico di Milano, Milan, Italy (e-mail: enrico.zio@ecp.fr, enrico.zio@supelec.fr, enrico.zio@polimi.it)

timely and efficient manner. Considering multiple types of infrastructure networks simultaneously, Kozin and Zhou [22] developed a Markov process to describe the process of infrastructure network recovery; then, they used dynamic programming to estimate the repair resources required for each time step and for each network, so as to maximize the expected economic return from system functioning. Noda [23] used a neural network to minimize the likelihood of post-earthquake functional loss for a telephone system. Bryson et al. [24] applied a mixed integer programming approach for selecting a set of recovery subplans giving the greatest benefit to business operation. Casari and Wilkie [25] discussed restoration when multiple infrastructures, operated by different firms, are involved. Lee et al. [26] focused on a case of network restoration that involves selecting the location of temporary arcs (e.g., shunts) needed to completely reestablish network services over a set of interdependent networks. A mixed-integer optimization model was proposed to minimize the operating costs involved in temporary emergency restoration. Xu et al. [27] applied a genetic algorithm to a problem associated with restoring power after an earthquake. The objective of this problem was the minimization of the average time that each customer stays without power (therefore, no prioritization is given to demand to critical points within the infrastructure). Finally, Matisziw et al. [28] propose an integer programming model to restore networks where the connectivity between pairs of nodes is the driving performance metric associated with the network.

The studies cited above involving the optimization of post-disaster CI restoration apply a variety of modelling approaches and focus on different aspects of the restoration strategy (e.g. the repair order of damaged components, where and how to allocate repair resources, and so on).

This paper provides a framework for properly selecting recovery actions in order to optimize the resilience of infrastructure networks. We focus on the optimal completion time of each failed component, in order to obtain insights about the importance that recovering each single component has in improving the resilience of the whole system; on the other hand, the duration of the repair of the failed components is not considered in this article (i.e. the repair action is assumed to be instantaneous). The performance of the network is measured in terms of the flows delivered to demand nodes.

A project-oriented perspective is taken to plan the process of recovery from a network disruption: that is, a set of repair tasks must be scheduled in an optimal way, so as to maximize the network resilience over a predefined recovery time horizon. The network resilience is quantified based on the computation of network flows, which are the outcome of another optimization (done by network operators).

The bi-level resilience optimization problem (ROP) is formulated within a mixed integer programming (MIP) framework. Although several commercial software packages, such as Cplex [45], can be used to solve the proposed MIP problem, the time required to solve the MIP formulation may impair its application to real-time post-disaster restoration activities for large-scale infrastructure networks. Therefore, a heuristic dispatching rule is here proposed, which seeks to determine a set of repair tasks to be completed, differently from traditional methods that simply focus on selecting an individual repair task to be processed.

The results of the application of the approach to a case study involving the 400kV French Power Transmission Network (FPTN400) demonstrate that the scheduling rule is able to provide near-optimal solutions with much less computational cost than a classical approach to MIP solution based on a branch and cut algorithm [52], with potential for real-time restoration activities management.

The remainder of the paper is organized as follows. In Section II, we first discuss related literature works concerning the definition and measurement of resilience in the domain of systems engineering; then, we propose a novel quantitative definition of system resilience. Section III proposes a framework for selecting recovery actions for optimizing the resilience of infrastructure networks: in particular, the mathematical formulation of the resilience optimization problem is firstly provided in Section III.*A*; then, Section III.*B* focuses on the heuristic dispatching rule that we propose to timely solve the problem. Section IV applies the developed optimization approach to a realistic case study and compares its efficiency to the Cplex MIP solver. Conclusions and future perspectives are given in Section V.

II. System resilience definition and assessment

A. Critical Review of Literature

Holling [10] introduced the notion of resilience to the scientific world and provided the first system-level definition. Subsequently, the concept developed independently in disciplines ranging from environmental research to materials science and engineering, sociology, psychology and economics, giving rise to a number of different definitions and classifications of resilience within these fields [15]. Yet, it is believed that the current strong interest in resilience for infrastructure systems has been triggered in the aftermath of 9/11 attacks [30].

One of the pioneering works in the field of infrastructure systems resilience is from the Multidisciplinary and National Center for Earthquake Engineering Research (MCEER) [12], where a general framework is provided to define and assess the seismic resilience of communities or any type of physical and organizational systems. This framework consists of “4Rs”: robustness, redundancy, resourcefulness, and rapidity, while resilience itself encompasses four interrelated dimensions: technical, organizational, social and economic.

Based on the general framework provided by Bruneau et al. [12], various studies have been carried out with the purpose of providing a practical interpretation of the concept of resilience and identifying possible ways of measuring it for giving support to resilience-based decisions. Most of these approaches to resilience interpretation and definition include aspects of a system withstanding disturbances, adapting to the disruption, and recovering from the state of reduced performance, and can rely upon a common concept which is illustrated schematically

in Fig. 1.

A quantifiable and time-dependent system performance function (also referred to system-level delivery function or figure-of-merit) $F(t)$ is the basis for the assessment of system resilience. It has a nominal value $F(t_0)$ under nominal operating conditions. The system operates at this level until suffering a disruptive event at time t_e. The disruption generally deteriorates system performance to some level $F(t_d)$ at time t_d. Then, recovery is started for increasing back system performance until a targeted level $F(t_r)$ is achieved once recovery is completed ($F(t_r)$ could be the same (as in Fig. 1), lower or higher than the original system performance level $F(t_0)$). The dotted curve in Fig. 1 denotes the targeted system performance $TF(t)$ if not affected by disruption. It is noted that various strategies exist for recovery activities, and system performance is ultimately a function of recovery decisions and actions. The period $t_d \leq t \leq t_r$ is generally considered as the recovery time [9].

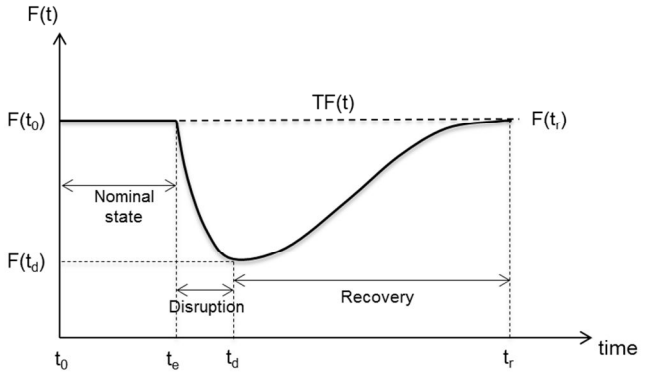


Fig. 1. Generic system performance transition curve under the occurrence of a disruptive event.

Many studies in the literature define and measure resilience based only on initial system losses caused by disaster. Najjar and Gaudiot [32] regard network resilience as a measure of network fault tolerance in a multicomputer system: in this framework, network resilience $NR(p)$ represents the upper bound on the number of node failures allowed, and is defined as the maximum number of node failures that can be sustained while the network remains connected with a probability $(1 - p)$. Omer et al. [33] suggest a model to measure resilience of a telecommunication cable system as a network infrastructure. The ratio of the "value delivery" of the network after a disruption to that before a disruption is defined as a reference for resilience, where "value delivery" is the amount of information that has to be carried through the network. Rosenkrantz et al. [34] identify resilience metrics for service-oriented networks, where edge resilience of a network is defined as the largest value k such that, no matter which subset of k or fewer edges fail, the residual sub-network is self-sufficient. Node resilience is also defined in the same manner.

These definitions focus on the static "survival" property of a system, measuring the degree of system performance after a disruption. They largely overlap with the existing concepts of fault tolerance and robustness, while the temporal dimension of post-disaster loss recovery (i.e. the time $t > t_d$ in Fig. 1) is not considered: on the other hand, this time period is significant for evaluating the system ability to leap back from disruption.

For this reason, other works have considered the system ability to recover from disruption. For example, MCEER [12] proposes that the seismic resilience of a community to an earthquake can be measured by the area between $F(t)$ and $F(t_0)$. Cimellaro et al. [9] attempt to formulate a framework to quantify system resilience under seismic risk, taking into account both the losses due to the disaster and the recovery phase. They view system resilience as the area underneath the performance function $F(t)$ of a system, normalized by a control time t_{LC}. Ouyang and Dueñas-Osorio [35] introduce a time-dependent resilience metric for infrastructure systems, where system resilience is quantified as the ratio of the area included between $F(t)$ and the time axis to the area included between $TF(t)$ and the time axis. The time span considered here is from t_0 to a sufficiently large $t(t > t_r)$ that allows future system evolution: this metric explicitly embraces the system failure process.

Vulgrin et al. [31] develop a composite resilience measure Z that simultaneously considers recovery of system performance and the resource expenditures required to achieve it. Two key quantities are computed: (i) the so-called systemic impact (SI) (defined as the cumulative impact of decreased system performance following a disruption and graphically represented by the area between the targeted system performance $TF(t)$ and the actual system performance $F(t)$) and (ii) the total recovery effort (TRE) (defined as the cumulative resources expended in recovery activities). However, the disadvantage of this approach is that an increase in SI and TRE implies an increase in its composite resilience measure Z ($Z = SI + \alpha\, TRE$), rather than a decrease.

Henry and Ramirez-Marquez [15] attempt to review different definitions and metrics for system resilience, and introduce a resilience metric referring to the basic meaning of the word "resilience". They view resilience $R(t)$ as the ratio of recovery to loss at a given time t, measured by $R(t) = \frac{F(t)-F(t_d)}{F(t_0)-F(t_d)}$. This formulation is identical to Rose's [36] static resilience metric when $F(t_d)$ is taken to be Rose's worst-case quantity. Henry and Ramirez-Marquez [15], then, apply this measure to various scenarios that disable links in a transportation network in order to find restoration sequences that maximize recovery at a given time. However, this metric itself does not embrace the integral temporal dimension of the recovery process, thus neglecting the speed with which the performance of the system is recovered.

B. System Resilience Definition and Assessment in This Work

In light of the issues highlighted above, we propose a new metric for analytical quantification of the resilience of infrastructure systems. It is still relying on the basic meaning of the word "resilience" and can be applied to evaluate and compare the effectiveness of different strategies that are proposed to reduce adverse consequences of disruptive events.

Let $R(t)$ be the resilience of a system at time t ($t \geq t_d$). In its basic form, $R(t)$ is here given the meaning of the cumulative

system functionality that has been restored at time t, normalized by the expected cumulative system functionality during this same time period. Graphically, $R(t)$ is represented by the ratio of the area with diagonal stripes S_1 to the area of the shaded part S_2, as illustrated in Fig. 2. Mathematically, it is given as:

$$R(t) = \frac{\int_{t_d}^{t}[F(\tau)-F(t_d)]d\tau}{\int_{t_d}^{t}[TF(\tau)-F(t_d)]d\tau}, t \geq t_d \quad (1)$$

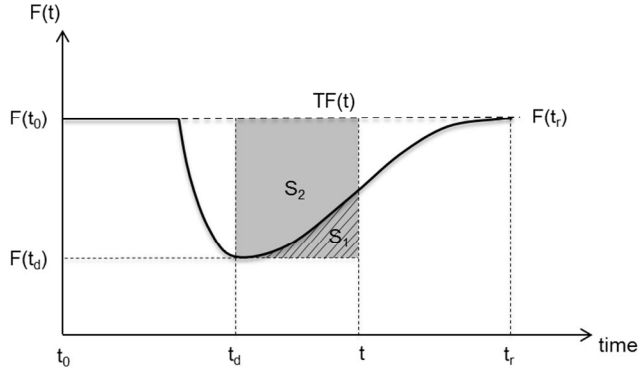


Fig. 2. Conceptual illustration of the proposed resilience metric $R(t)$

The following considerations about the given resilience definition are important:

1) The system resilience $R(t)$ defined in Eq. (1) measures the cumulative system performance that has been restored from the system disrupted state to the recovered state at current time t, normalized by the target cumulative performance as if the system were not affected by disruption. This formulation is aligned with the original meaning of the concept of resilience, while capturing at the same time both the magnitude and rapidity of the system recovery action.

2) The system performance function $F(t)$ could be represented by different metrics (e.g., the amount of flow or services delivered, the availability of critical facilities, the number of customers served, or the enabling potential of economic activities for infrastructure systems), depending on which dimension (i.e., technical, organizational, social and economic) of resilience the analysis focuses on [12]. This study concentrates on the technical dimension of resilience and utilizes the amount of flow delivered to the demand nodes of a network as the performance level metric.

3) Note that $R(t)$ is undefined when $F(t_d) = TF(t)$, which means that a system does not suffer any loss. This condition is avoided since only systems exposed to disruptive events are here considered. Practically, if a system does not suffer any loss, there is no scope for it to be recovered or to bounce back and thus there is no need to evaluate resilience.

4) $R(t)$ is undefined when $t < t_d$, because of the same reason explained in item 3. Besides, this could avoid any overlap with existing concepts like robustness, vulnerability and survivability.

5) $R(t) \in [0, 1]$ and $R(t) = 0$ when $F(t) = F(t_d)$, which means that a system has not recovered from its disrupted state (i.e. there has been no "resilience" action); $R(t) = 1$ when $F(t) = TF(t)$, which corresponds to the ideal case where a system recovers to its target state immediately after disruption.

6) The target system performance $TF(t)$ is generally evolving due to the dynamic nature of service demand in infrastructure systems. For simplicity, in this study we assume that $TF(t)$ equals $F(t_0)$ and remains invariant.

III. Optimal Recovery of Post-Disaster Infrastructure Networks

After the definition of system resilience, we focus on the role of various recovery decisions and actions in the task of optimizing the resilience of infrastructure networks subject to disruptive events. In this Section, we first formulate a general resilience optimization model for infrastructure networks; then, we propose a heuristic dispatching rule for its practical solution.

A. Resilience Optimization Model

The mathematical model for the resilience optimization problem here considered involves an infrastructure network $G(V, E)$ comprising a set of nodes V connected by a set of links E. The network nodes are classified into supply nodes V_S, transshipment nodes V_T, and demand nodes V_D ($V_S \cup V_T \cup V_D = V$). Each arc $(i, j) \in V$ has an associated capacity $(i, j) \in \boldsymbol{R}_0^+$, while each supply node $i \in V_S$ has a supply capacity per time unit $P_i^s \in \boldsymbol{R}_0^+$ and each demand node $j \in V_D$ has a demand $P_j^D \in \boldsymbol{R}_0^+$ per time unit. Network flow is sent from supply nodes to demand nodes respecting the flow capacities of the links and supply/demand capacities of the nodes. Each unit of flow that arrives at demand node $j \in V_D$ is given a weight $w_j \in \boldsymbol{Z}^+$ in order to differentiate priorities of demand nodes (e.g., a hospital usually has a higher weight than a residential household in a power network). The performance of the network is evaluated by determining the maximum amount of weighed flow that can be received by the demand nodes. Formally, the system performance function is defined as:

$$F(t) = \sum_{j \in V_D} w_j f_j(t) \quad (2)$$

where $f_j(t)$ represents the amount of flow received by demand node j at time t.

Disruptions happen and create damages to nodes and/or links in the network, as modeled by the removal of a subset of arcs, $E' \subset E$.[1] The arcs in set E' are viewed as non-operational immediately after the disruption. System performance $F(t)$ achieve its minimum value at this time ($t = 0$, i.e. $F_{min} = F(0)$).

In a recovery optimization framework, we are not only interested in identifying a subset of the links in E' to be installed to the disrupted network, but also in selecting an optimal order of installation and repair of these links. The goal is to achieve maximum system resilience over the whole restoration horizon $T \in \boldsymbol{Z}^+$. Link repairs are here assumed to be

[1] If nodes are important in a specific application problem, they can be converted to equivalent arcs by introducing additional arcs and nodes into the network, i.e. by 'splitting' a node into two nodes and an arc.

discrete tasks, and a repair cost $\beta(i,j) \in \boldsymbol{Z}_0^+$ is associated to each arc $(i,j) \in E'$. The processing time of a single arc restoration is not considered in this study (i.e., the repair action is assumed to be instantaneous); instead, the main focus is when the disrupted arcs should come back online. In addition, the number of arcs that can be restored in each time period is constrained by their total cost. By combining Eqs. (1) and (2), system resilience to be maximized at time T is given by

$$R(T) = \frac{\sum_{t=1}^{t=T}\left[\sum_{j\in V_D} w_j f_j(t) - F_{min}\right]}{T\cdot\left(\sum_{j\in V_D} w_j P_j^D - F_{min}\right)}. \quad (3)$$

The optimization variables of the resilience optimization problem include: (i) continuous variables $f_{ij}(t) \in \boldsymbol{R}_0^+$, $(i,j) \in E$ and $t = 1, \dots, T$, that denote the flows moving from node i to node j through link (i,j) at time unit t; (ii) continuous variables $f_j(t) \in \boldsymbol{R}_0^+$, $j \in V_D$, that represent the amounts of flow received by demand node j at time unit t, and (iii) binary state variables $s_{ij}(t)$, $(i,j) \in E$ and $t = 1, \dots, T$, such that $s_{ij}(t) = 1$ if arc (i,j) is operational and $s_{ij}(t) = 0$ if arc (i,j) is not operational at time unit t.

We are interested in optimizing the resilience over the whole restoration process: thus, the timespan T is chosen as the total recovery time, defined as the period necessary to restore the system functionality to the same level as the original system. Consequently, the formulation of the resilience optimization problem is as follows:

$$\max \quad \frac{\sum_{t=1}^{t=T}\left[\sum_{j\in V_D} w_j f_j(t) - F_{min}\right]}{T\cdot\left(\sum_{j\in V_D} w_j P_j^D - F_{min}\right)} \quad (4)$$

Subject to:

$$\sum_{(i,j)\in E} f_{ij}(t) - \sum_{(j,i)\in E} f_{ji}(t) \le P_i^S, \forall i \in V_S, t = 1, \dots, T \quad (5)$$

$$\sum_{(i,j)\in E} f_{ij}(t) - \sum_{(j,i)\in E} f_{ji}(t) = 0, \forall i \in V_T, t = 1, \dots, T \quad (6)$$

$$\sum_{(i,j)\in E} f_{ij}(t) - \sum_{(j,i)\in E} f_{ji}(t) = -f_j(t), \ \forall i \in V_D, t = 1, \dots, T \quad (7)$$

$$0 \le f_j(t) \le P_j^D, \forall i \in V_D, t = 1, \dots, T \quad (8)$$

$$0 \le f_{ij}(t) \le s_{ij}(t) P(i,j), \forall (i,j) \in E, t = 1, \dots, T \quad (9)$$

$$s_{ij}(t) \le s_{ij}(t+1), \forall (i,j) \in E, t = 1, \dots, T \quad (10)$$

$$\sum_{(i,j)\in E'} \beta(i,j)\left[s_{ij}(t) - s_{ij}(t-1)\right] \le C(t), \forall t = 1, \dots, T \quad (11)$$

$$s_{ij}(t) \in \{0,1\}, s_{ij}(0) = 0, \forall (i,j) \in E, t = 1, \dots, T \quad (12)$$

The objective (4) is to maximize the system resilience over the time horizon of the problem. Constraints (5)-(9) are typical network flow constraints over the links and supply/demand nodes in the network in period t. They ensure that: (i) the flow generated at a supply node does not exceeds its supply capacity (5); (ii) the amount of net injected flow at a transshipment node is zero (6); (iii) the amount of net injected flow at a demand node is equal to the received flow at the node (7) while not exceeding its requested demand (8); (iv) the flow on an operational link does not exceed its capacity and there is no flow passing through an arc if the arc has not been repaired (9); constraint (10) ensures that once an arc has been restored at time t, it will keep operational thereafter; finally, constraint (11) ensures that the total cost paid for repairing links in a time period does not exceeds the available resources that can be allocated in this period.

B. Dispatching Rule for ROP Solution

The resilience optimization problem (ROP) introduced before is a mixed (binary) integer programming (MIP) problem, which has $O(|E|\cdot T + |V_D|\cdot T)$ continuous variables, $O(|E|\cdot T)$ binary variables and $O(|V|\cdot T + |E|\cdot T + 2|E'|\cdot T)$ constraints. It has been proven to be strongly NP-complete [38] and, thus, it is computationally intense especially for large-scale infrastructure networks composed of thousands of nodes and links.

It is noted that the evaluation of a potential solution to the ROP (i.e. of a scheduled set of recovery actions on the disrupted links) requires evaluating the state of the system at a given time, i.e. calculating the network flows, which is the result of a lower-level network flow optimization. This bi-level optimization structure differentiates the ROP from other resource-constrained project scheduling problems (RCPSP) extensively described in the literature [37], [38]: these are generally based on the criterion of minimizing the makespan (the time to project completion) whose calculation is trivial. Consequently, many existing meta-heuristic algorithms for RCPSP such as genetic algorithms [39], simulated annealing [40], particle swarm [42] and ant colony optimization [41] are most likely unable to solve the ROP without incurring in a large penalty in computational expense.

On the other hand, there has been a significant amount of studies in RCPSP proposing some so-called dispatching rules, which usually characterize the profitability of scheduling a certain task by evaluating its contribution to the objective function and then greedily schedule the unscheduled tasks with the best profitability [38].

The key point in designing a heuristic dispatching rule for our ROP is to understand how restoring an arc impacts the objective function Eq. (3) of the problem. In this view, a straightforward idea is to modify the classical weighed shortest processing time (WSPT) first rule [43] by selecting the arc to be restored as the one that maximizes the ratio of the improvement of system resilience and the cost of restoring the arc. However, this approach is short-sighted in the sense that some links will not enhance the system resilience (i.e. will not increase the amount of flow received by demand nodes) if they are not restored in a given predefined sequence with other transmission links. Thus, the profitability of restoring a *set* of arcs instead of a *single* arc is taken into account in designing our dispatching rule.

It is well known that the residual network associated with a maximum network flow does not contain an augmenting path from the supply node to the demand node [44]. In this view, in order to increase the amount of flow received by the demand nodes in the current operational network after a disruptive event, a set of links forming some residual paths that have the potential to augment the flow received by the demand nodes must be restored. The main idea of our dispatching rule for the ROP is, then, to select a set of unrepaired links that belong to some residual path and that maximize the ratio of the potential

augmented flow received by the demand nodes to the cumulative cost of repairing all the uninstalled links in this path. The potential augmented flow received by demand nodes is further limited by the following three elements: the residual capacity of the path, the residual capacity of the supply node and the unmet flow of the demand node.

Mathematically, suppose that $G_t(V, E_t)$ is a partially restored network at time t, X^* is the optimal flow (the result of the lower-level network flow optimization) associated with $G_t(V, E_t)$. The links in $G_t(V, E_t)$ will, then, have a residual capacity $rp(i,j) = P(i,j) - f_{ij}(t),\ \forall (i,j) \in E_t$ and repair cost $\beta(i,j) = 0, \forall (i,j) \in E_t$, since they are already operational. The supply and demand nodes in $G_t(V, E_t)$ will have a residual capacity $RP_i^S = P_i^S - f_i(t),\ \forall i \in V_S$ and unmet demand $RP_j^D = P_j^D - f_j(t),\ \forall j \in V_D$, respectively. The unrestored links in the disrupted link set E' have a residual capacity equivalent with their original capacity $P(i,j)$, and a repair cost $\beta(i,j)$. Then, the residual capacity of path $P_{s\to d}$ from supply node s to demand node d is defined as $R(P_{s\to d}) = \min_{(i,j)\in P_{s\to d}} rp(i,j)$. The cumulative cost of repairing all the uninstalled links in path $P_{s\to d}$ is $\sum_{(i,j)\in P_{s\to d}} \beta(i,j)$. Then, we are interested in selecting the uninstalled links in the path to be repaired, that is an optimal solution to the following problem:

$$\max_{P_{s\to d}\in \aleph} \frac{\min\ \{RP_s^S, RP_d^D, R(P_{s\to d})\}\cdot w_d}{\sum_{(i,j)\in P_{s\to d}} \beta(i,j)} \tag{13}$$

where $\aleph$ is the set of all paths from all supply nodes to all demand nodes in the original network $G(V, E)$. The numerator of formula (13) provides a measure of the potential augmented (weighted) flow received at demand node d by restoring path $P_{s\to d}$ while the denominator measures the cost required to restore all disrupted links in path $P_{s\to d}$.

In order to determine an optimal path to (13), we suppose that $\gamma(P_{m\to n}) \cdot w_n$ is the numerator in an optimal solution to (13), i.e. $\gamma(P_{m\to n}) = \min\ \{RP_m^S, RP_n^D, R(P_{m\to n})\}$; then, $P_{m\to n}$ is the path with the lowest cost in the network where we only include links whose residual capacities are greater than or equal to $\gamma(P_{m\to n})$. This leads to an algorithm to solve (13): for each potential value of the numerator (including each potential value of the residual capacity of a path, each residual capacity of supply nodes and each unmet flow of demand nodes), we determine the minimum cost path in the network comprising only these links whose residual capacities are larger than the numerator. The minimum cost path can be obtained by first constructing a weighed network, where the link weights are set as their repair costs and, then, searching the shortest path on the weighed network constructed. We can, then, obtain an optimal solution in this procedure by marking the path that has the maximum value of ratio (13). It is noted that the residual capacity of a path is the minimum residual capacity of the links in the path, so there are at most $(|V_S| + |V_D| + |E|)$ different values to be considered, which means the next sets of links to be restored can be determined by solving $O(|V_S| + |V_D| + |E|)$ shortest path problems.

TABLE I
ALGORITHM FOR PATH SELECTION IN THE DISPATCHING RULE

Input: Residual capacity $R(i,j)$ for each of the links $(i,j) \in E$, residual capacity RP_i^S for each supply node $i \in V_S$, unmet demand RP_j^D and flow weight w_d for each demand node $j \in V_D$ in the current network $G_t(V, E_t)$ associated with an optimal flow X^*

Set $GlobalRatio = 0$, $\boldsymbol{P}$ = null.

Sort the set $\{R(i,j)\ RP_i^S\ RP_j^D\}$ in non-increasing order to obtain an ordered composite set $\boldsymbol{R}$

for each $r \in \boldsymbol{R}$

  Construct a weighted network G^* including only the links, where $R(i,j) \geq r$. The weight of a link is set as $\beta(i,j)$ if it is a non-restored link; set the weight as 0 if it is an operational link

  for each $i \in V_S$ and $j \in V_D$

    Find the shortest weighed path $P_{i\to j}^*$ from i to j in the network G^*, calculate the path length $d(P_{i\to j}^*) = \sum_{(i,j)\in P_{i\to j}^*} \beta(i,j)$

    if $\frac{\min\ \{RP_i^S, RP_j^D, R(P_{i\to j}^*)\}\cdot w_d}{d(P_{i\to j}^*)} > GlobalRatio$

      $GlobalRatio = \frac{\min\ \{RP_i^S, RP_j^D, R(P_{i\to j}^*)\}\cdot w_d}{d(P_{i\to j}^*)}$

      $\boldsymbol{P} = P_{i\to j}^*$

    end if

  end for

end for

Return $\boldsymbol{P}$

Formally, we provide the pseudo code of the algorithm for path selection in our dispatching rule in Table I. We assume that the residual network $G_t(V, E_t)$ associated with an optimal flow X^* at a given time t has been calculated as part of the inputs of the algorithm. Other inputs include the residual capacity $R(i,j)$ for each link $(i,j) \in E$, the residual capacity RP_i^S for each supply node $i \in V_S$, and the residual capacity RP_j^D and flow weight w_d for each demand node $j \in V_D$. The variable $GlobalRatio$ flags the current optimal ratio in formula (13). The output of the algorithm is a path composed of the next set of arcs that should be restored to the network.

After obtaining the next set of links to be restored by applying the algorithm introduced above, we can easily allocate these link repair tasks into each timeslot subject to constraint (11), until all links from this set are restored. The link repair order within this set is not significant since we assume that a link repair task can be split into two timeslots. Therefore, we

can view this set of links as a queue and we will restore the next link in the queue once the previous task is finished. If no links are in the queue, we will determine the next set of links to be restored by considering the residual network associated with an optimal solution to the lower-level maximum flow problem, where all links that have been restored are regarded as operational in the network. This process continues until either all links are restored or the end of the time horizon is reached. In the Appendix we illustrate the detailed steps of the proposed algorithm by applying it to a very simple network.

IV. Case Study

We will now discuss the results obtained by applying the ROP to a realistic infrastructure network system, i.e. the 400kV French Power Transmission Network (FPTN400) (See Fig. 3). We are particularly interested in examining the performance of the proposed heuristic dispatching rule in the network and to this aim we compare the results with those obtained with a widely used commercial optimizer – Cplex [45]. Testing calculations are performed on a double 2.4 GHz Intel CPU and 4 GB RAM computer.

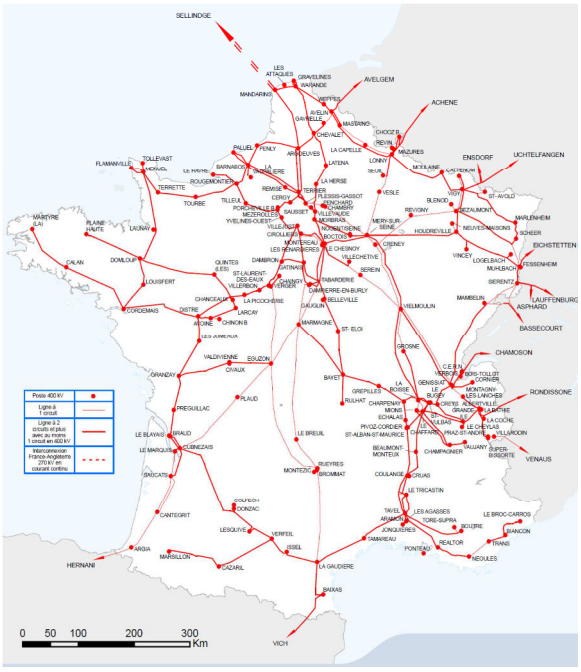


Fig. 3. The 400kV French Power Transmission Network (FPTN400) [46]

The FPTN400 data on the 400 kV transmission lines is taken from the RTE website [46]. The network has 171 nodes (substations) and 220 edges (transmission lines). We distinguish the generators, which are the sources of power, from the other distribution substations, that receive power and transmit it to other substations or distribute it in local distribution grids. By obtaining the power plants list from EDF website [47] and relating them with the ID of the buses in the transmission network, we have 26 generators and 145 distributors. Only the nuclear power plants, hydroelectric plants and thermal power plants whose installed capacities are larger than 1000 MW, are considered.

The supply capacities of the generators in the FPTN400 are approximated to their installed capacities, taken from EDF website [47]. Capacity limits of transmission lines are obtained from European Commission [48]. Since there is no sufficient public information about loading of particular substations, in order to estimate the load level we have assumed that demand levels are directly related to the local population and industry [49]. Specifically, the total demand of the country is distributed into groups of demands by administration areas (i.e. provinces), whose population can be obtained at the website Consulting V. [51]; then, for simplicity the load buses in each region are assumed to share equally the regional load.

In the case study, we randomly select parts of arcs in the network to be damaged. In addition, the repair costs of all the transmission lines are assumed to be constant and identical, and the cost limits $C(t)$ are assumed to be equal to the repair cost of a single arc: this means that only a single arc can be repaired at any given timeslot. It is noted that these assumptions can be relaxed to adapt to more realistic application cases.

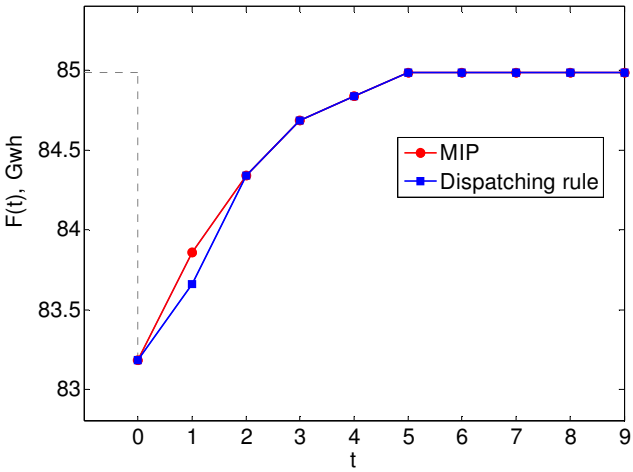


Fig. 4. Optimal restoration curves obtained by the dispatching rule and MIP solver for the specific disruption scenario (10% links damaged) on the FPTN400.

We firstly consider repair optimization for a specific disruption scenario on the FPTN400, where 10% of network arcs (i.e. 22) are initially damaged. All the demand nodes are assumed to have identical weights in the optimization process. For the solution of the repair optimization problem, both the heuristic dispatching rule and MIP solver are applied. Fig. 4 reports the optimal restoration curves obtained by the dispatching rule (squares) and MIP (circles), respectively. It is found that the dispatching rule is able to obtain near optimal solutions: the recovery duration T is 5 (in arbitrary units) for both methods, and the system resilience R (Eq. 3) is $R_{disp} = 0.731$ for the dispatching rule, and $R_{opt} = 0.753$ for MIP: the optimality gap between the two approaches is only 2.92%. Fig. 5 provides a visualization of the optimal recovery plans obtained by the two methods. It is shown that the dispatching rule achieves very similar restoration plans to that of MIP. Both cases give high repair priority to those transmission lines which are unique connections to the demand nodes. More importantly, the dispatching rule is computationally much cheaper (6.9s)

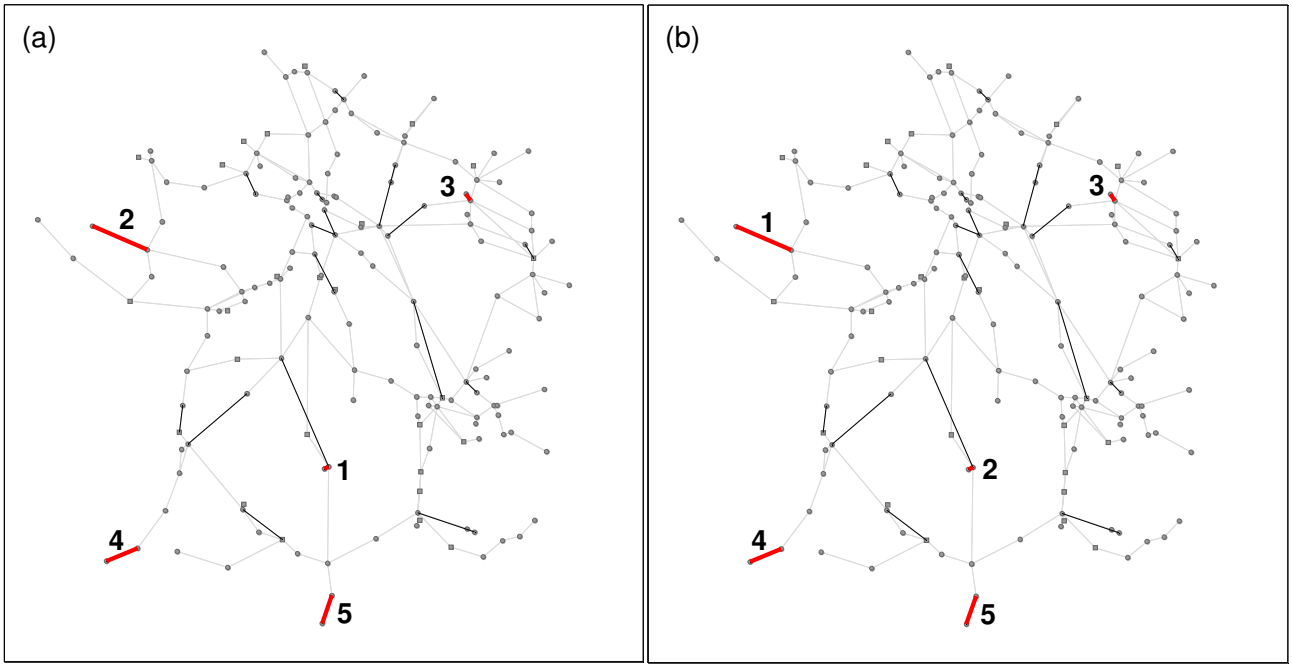


Fig. 5. Visualization of the optimal recovery plans obtained by the dispatching rule (a) and MIP solver (b) for the specific disruption scenario (10% links damaged) on the FPTN400. The numbers indicate the optimal recovery timeslots of the five arcs marked by bold solid lines; black lines correspond to other failed arcs.

TABLE II
PERFORMANCES OF THE HEURISTIC DISPATCHING RULE AND THE CPLEX MIP SOLVER ON THE FPTN400

% of failed arcs (number)	w_j	Heuristic dispatching rule				Cplex MIP solver		
		Recovery time T	Opt. resilience	Solver time (s)	Opt. gap (%)	Recovery time T	Opt. resilience	Solver time (s)
5% (11)	Constant	2	0.917	4.69	4.28	2	0.958	20.30
5% (11)	Priority	2	0.921	4.75	6.40	2	0.984	20.94
10% (22)	Constant	5	0.731	6.90	2.92	5	0.753	40.50
10% (22)	Priority	5	0.852	8.60	0.00	5	0.852	46.32
15% (33)	Constant	14	0.646	20.45	5.42	12	0.683	110.16
15% (33)	Priority	14	0.685	26.40	13.07	12	0.788	224.45
20% (44)	Constant	15	0.569	70.31	9.97	13	0.632	632.42
20% (44)	Priority	15	0.626	75.46	8.08	13	0.681	1102.80

than MIP (20.5s).

In order to further demonstrate the performance of the heuristic dispatching rule, we considered different levels of damage on the network (5% to 20% of arcs are randomly selected to be failed) and two different types of weights for the demand nodes (i.e. w_j for $j \in V_D$): in the first class of demand nodes weights (namely, "Constant") each unit of flow received by demand nodes is weighed evenly across all the demand nodes; in the second class ('Priority'), some randomly chosen demand nodes are assigned higher value of w_j to represent higher priority. Table II provides the solutions and corresponding computational performances of the heuristic dispatching rule and the Cplex MIP solver for the ROP on the FPTN400. It is shown that the recovery time T provided by the heuristic dispatching rule is the same (for 5% and 10% cases) or slightly larger (for 15% and 20% cases) than the optimal solutions, and the relative optimality gaps between the two methods are less than 10% in most cases. Furthermore, the dispatching rule needs only, on average, the 10% of the computation time needed by the MIP solver for all the cases. These results indicate that the proposed heuristic dispatching rule is able to obtain high-quality sub-optimal (and optimal in some cases) solutions to the ROP, with much less computational cost compared with the Cplex MIP solver.

It is noted that the MIP solver may need much more time (e.g., days) to achieve optimal solutions for larger infrastructure systems (e.g., composed of thousands of nodes and links) or heavier disruption events (e.g., over 20% components damaged). Thus, it is unreasonable to expect the managers of the infrastructure systems to have access to unlimited computing resources or be willing to wait for several hours (or even several days) to determine their restoration plan. Consequently, the proposed heuristic dispatching rule represents an appealing tool for real-time restoration activities on larger-scale CI systems.

V. CONCLUSIONS AND FUTURE WORKS

In this study, we have firstly reviewed different definitions of

system resilience and different metrics to evaluate it in the context of systems engineering, especially for infrastructure network systems. Then, we have proposed a novel time-dependent metric of system resilience focusing on the post-disaster recovery process. This metric is consistent with the basic meaning of resilience and it is able to quantify how a system "bounces back" from a disrupted state to an accepted performance.

Based on this resilience definition, we have then provided a framework for considering the role of recovery decisions and actions in the resilience optimization of infrastructure networks. Specifically, a project-oriented perspective has been applied to plan the process of network recovery after a disruptive event: that is, a set of link repair actions must be scheduled in an optimal way so as to maximize the network resilience over the recovery time. This resilience optimization problem (ROP) has been formulated within a mixed integer programming (MIP) framework. Although several commercial optimizers such as CPLEX and Gurobi can be applied to obtain the MIP solution, the time required to solve the MIP formulation may impair their application for effective restoration activities after extreme events affecting large-scale infrastructure networks. Therefore, a heuristic dispatching rule that integrates fundamental concepts from network flows and project scheduling has been here proposed: differently from traditional approaches to recovery actions planning, it seeks to determine a *set* of repair tasks to be processed rather than an *individual* repair task. The application on a case study concerning the FPTN400 has shown that the proposed dispatching rule is able to obtain high-quality sub-optimal (and optimal in some cases) solutions to the ROP, with much less computational cost if compared with the widely adopted Cplex MIP solver: this provides impetus for the application of the heuristic dispatching rule to restoration activities on large-scale CI systems.

Future works will examine different methods to evaluate the performance of an infrastructure network, e.g. the integration of the DC power flow model [50] in the calculation of network flows (which may be more appropriate to model the operation of electrical infrastructures). Also, application of the resilience optimization framework and the proposed heuristic dispatching rule to larger and more complex infrastructures subject to realistic disruptive events will be considered in order to better demonstrate the effectiveness of the proposed dispatching rule. Besides, it will be interesting to explore an extension to a probabilistic scenario considering component restoration times (and costs) as random variables. Another important direction for future research is to explore other applications for the resilience metric introduced, e.g. to propose resilience-based component importance measures and their use in prioritizing restoration activities.

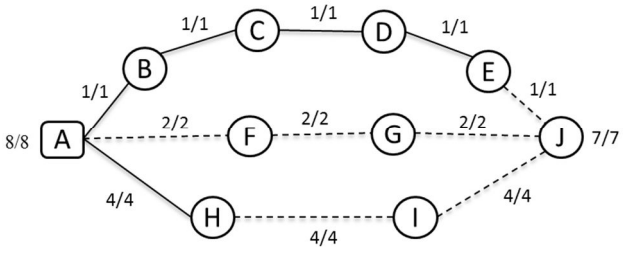


Fig. 6. A simple disrupted network; the dashed lines indicate failed arcs.

APPENDIX: A SIMPLE EXAMPLE FOR DISPATCHING RULE ILLUSTRATION

Consider the post-disaster network shown in Fig. 6 with supply node A, demand node J and transship nodes B to I. The dashed lines in the figure indicate the failed arcs immediately

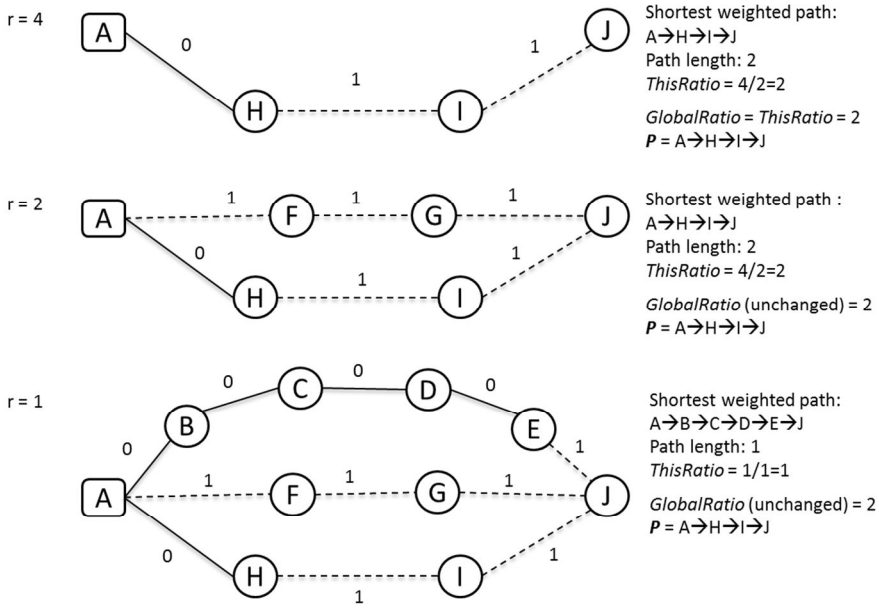


Fig. 7. Illustration of the execution process of the path selection algorithm in Table I on a simple network

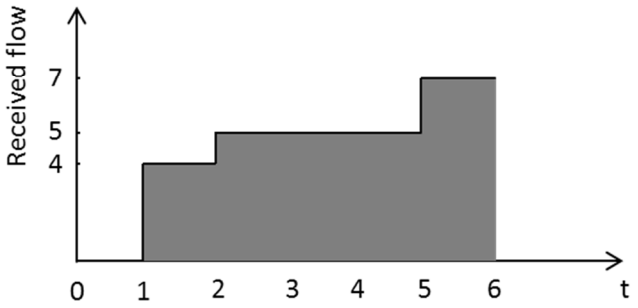


Fig. 8. Optimal restoration curve of the network performance

after a disruptive event ($t = 0$), where the links A-F, F-G, G-J, H-I, I-J, E-J are disrupted. The numbers $R(i,j)/P(i,j)$ associated with each arc in the Figure represent the residual capacity $R(i,j)$ of the arc at time 0 and the original capacity $P(i,j)$. Note that the residual capacity of a failed arc is regarded as its original capacity, rather than zero. Similarly, the numbers 8/8 associated with the supply node A represent its residual capacity $RP_A^S = 8$ and its original capacity $P_A^S = 8$; the numbers 7/7 associated with the demand node J represent its unmet demand $RP_I^D = 7$ and flow demand $P_I^D = 7$, respectively. Besides, the repair costs of all the arcs are assumed to be constant and set as 1. The performance of the network is evaluated by the flow received by demand node J.

The path selection algorithm in Table I, first sorts the residual capacity array $\{R(i,j)\ RP_i^S\ RP_j^D\}$ at current time ($t = 0$), resulting in a non-increasing set $\boldsymbol{R} = \{8, 7, 4, 2, 1\}$; then, for each value in the set, the algorithm executes step 4 to step 11, illustrated graphically in Fig. 7. Note that $r = 8$ and $r = 7$ are skipped since there is no weighed network associated to those two cases. The output of the execution $\boldsymbol{P} = \mathrm{A} - \mathrm{H} \rightarrow \mathrm{I} \rightarrow \mathrm{J}$ is the path that should be selected to be restored.

The network restoration is preceded by applying this path selection algorithm and then allocating these link repair tasks of the selected path into each timeslot subject to constraint (11). Assuming that only a single arc can be repaired at any given timeslot, we can obtain the optimal restoration curve of the network performance, as shown in Figure 8.

REFERENCES

[1] Lewis, T. G. (2006). *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley & Sons.

[2] Clinton, W. (1998). "Presidential Decision Directive PDD-63, Protecting America's Critical Infrastructures," Washington, D.C.

[3] Bush, G.W. (2002). "Homeland Security Presidential Directive-3 (HSPD-3)," Washington, D.C.

[4] Bush, G.W. (2003). "Homeland Security Presidential Directive-7 (HSPD-7)," Washington, D.C.

[5] Moteff, J. D. (2012). *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, Congressional Research Service.

[6] Pursiainen, C. (2009). "The challenges for European critical infrastructure protection," *European Integration*, 31(6), 721-739.

[7] Obama, B. (2013). "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience," Washington, D.C.

[8] Zio, E. (2009). "Reliability engineering: Old problems and new challenges," *Reliability Engineering & System Safety*, 94(2), 125-141.

[9] Cimellaro, G. P., Reinhorn, A. M., & Bruneau, M. (2010). "Framework for analytical quantification of disaster resilience," *Engineering Structures*, 32(11), 3639-3649.

[10] Holling, C. (1973). "Resilience and Stability of Ecological Systems," *Annual Review of Ecology and Systematics*, pp. 1-23.

[11] Fiksel, J. (2003). "Designing Resilient, Sustainable Systems," *Environmental Science and Technology*, 37(23), pp. 5330-5339.

[12] Bruneau, M., S. Chang, R. Eguchi, G. Lee, T. O' Rourke, A. Reinhorn, M. Shinozuka, K. Tierney, W. Wallace, and D. von Winterfeldt (2003). "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," *Earthquake Spectra*, 19, pp. 737-38.

[13] Rose, A., and S.-Y. Liao (2005). "Modeling Regional Economic Resilience to Disasters: A Computable General Equilibrium Analysis of Water Service Disruptions," *Journal of Regional Science*, 45, pp. 75-112.

[14] Reed, D. A., Kapur, K. C., & Christie, R. D. (2009). "Methodology for assessing the resilience of networked infrastructure," *Systems Journal, IEEE*, 3(2), 174-180.

[15] Henry, D., & Emmanuel Ramirez-Marquez, J. (2012). "Generic metrics and quantitative approaches for system resilience as a function of time," *Reliability Engineering & System Safety*, 99, 114-122.

[16] Park, J., T. P. Seager, P. S. C. Rao, M. Convertino, and I. Linkoz (2013). "Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems," *Risk Analysis*, 33(3), pp. 356-366.

[17] Shinozuka M, Chang SE, Cheng T, Feng M, O'Rourke T, Saadeghvaziri M, Dong X, Jin X, Wang Y, Shi P. (2004). "Resilience of integrated power and water systems," *MCEER Research Progress and Accomplishment 2003–2004*, Multidisciplinary Center for Earthquake Engineering Research, Buffalo, NY, pp. 65–86.

[18] Liu, H., Davidson, R. A., & Apanasovich, T. (2007). "Statistical forecasting of electric power restoration times in hurricanes and ice storms," *Power Systems, IEEE Transactions on*, 22(4), 2270-2279.

[19] Ferrario, E., & Zio, E. (2014). "Assessing nuclear power plant safety and recovery from earthquakes using a system-of-systems approach," *Reliability Engineering & System Safety*, 125, 103-116.

[20] Buzna, L., Peters, K., Ammoser, H., Kühnert, C., & Helbing, D. (2007). "Efficient response to cascading disaster spreading," *Physical Review E*, 75(5), 056107.

[21] Çağnan, Z., Davidson, R. A., & Guikema, S. D. (2006). "Post-earthquake restoration planning for Los Angeles electric power," *Earthquake Spectra*, 22(3), 589-608.

[22] Kozin, F., & Zhou, H. (1990). "System study of urban response and reconstruction due to earthquake," *Journal of Engineering Mechanics*, 116(9), 1959-1972.

[23] Noda, S. (1993). "Optimum post-earthquake restoration of a telephone system using neural networks," *Journal of natural disaster science*, 15(1), 91-111.

[24] Bryson, K. M. N., Millar, H., Joseph, A., & Mobolurin, A. (2002). "Using formal MS/OR modeling to support disaster recovery planning," *European Journal of Operational Research*, 141(3), 679-688.

[25] Casari, M., & Wilkie, S. J. (2005). "Sequencing lifeline repairs after an earthquake: an economic approach," *Journal of Regulatory Economics*, 27(1), 47-65.

[26] Lee, E. E., Mitchell, J. E., & Wallace, W. A. (2007). "Restoration of services in interdependent infrastructure systems: A network flows approach," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 37(6), 1303-1317.

[27] Xu, N., Guikema, S. D., Davidson, R. A., Nozick, L. K., Çağnan, Z., & Vaziri, K. (2007). "Optimizing scheduling of post-earthquake electric power restoration tasks," *Earthquake engineering & structural dynamics*, 36(2), 265-284.

[28] Matisziw, T. C., Murray, A. T., & Grubesic, T. H. (2010). "Strategic network restoration," *Networks and Spatial Economics*, 10(3), 345-361.

[29] Aven, T. (2011). "On some recent definitions and analysis frameworks for risk, vulnerability, and resilience," *Risk Analysis*, 31(4), 515-522.

[30] Haimes, Y. Y., Crowther, K., & Horowitz, B. M. (2008). "Homeland security preparedness: balancing protection with resilience in emergent systems," *Systems Engineering*, 11(4), 287-308.

[31] Vugrin, E. D., Warren, D. E., Ehlen, M. A., & Camphouse, R. C. (2010). "A framework for assessing the resilience of infrastructure and economic systems," In *Sustainable and Resilient Critical Infrastructure Systems* (pp. 77-116). Springer Berlin Heidelberg.

[32] Najjar, W., & Gaudiot, J. L. (1990). "Network resilience: a measure of network fault tolerance," *Computers, IEEE Transactions on*, 39(2), 174-181.

[33] Omer, M., Nilchiani, R., & Mostashari, A. (2009). "Measuring the resilience of the trans-oceanic telecommunication cable system," *Systems Journal, IEEE*, 3(3), 295-303.

[34] Rosenkrantz, D. J., Goel, S., Ravi, S. S., & Gangolly, J. (2009). "Resilience metrics for service-oriented networks: A service allocation approach," *Services Computing, IEEE Transactions on*, 2(3), 183-196.

[35] Ouyang, M., & Dueñas-Osorio, L. (2012). "Time-dependent resilience assessment and improvement of urban infrastructure systems," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 22(3), 033122.

[36] Rose, A. (2007). "Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions," *Environmental Hazards*, 7(4), 383-398.

[37] Brucker, P., Drexl, A., Möhring, R., Neumann, K., & Pesch, E. (1999). "Resource-constrained project scheduling: Notation, classification, models, and methods," *European journal of operational research*, 112(1), 3-41.

[38] Pinedo, M. L. (2012). *Scheduling: theory, algorithms, and systems*. Springer.

[39] Hartmann, S. (1998). "A competitive genetic algorithm for resource-constrained project scheduling," *Naval Research Logistics (NRL)*, 45(7), 733-750.

[40] Bouleimen, K., & Lecocq, H. (2003). "A new efficient simulated annealing algorithm for the resource-constrained project scheduling problem and its multiple mode version," *European Journal of Operational Research*, 149(2), 268-281.

[41] Merkle, D., Middendorf, M., & Schmeck, H. (2002). "Ant colony optimization for resource-constrained project scheduling," *Evolutionary Computation, IEEE Transactions on*, 6(4), 333-346.

[42] Jarboui, B., Damak, N., Siarry, P., & Rebai, A. (2008). "A combinatorial particle swarm optimization for solving multi-mode resource-constrained project scheduling problems," *Applied Mathematics and Computation*, 195(1), 299-308

[43] Smith, W. E. (1956). "Various optimizers for single-stage production," *Naval Research Logistics Quarterly*, 3(1-2), 59-66.

[44] Ahuja, R. K., Magnanti, T. L., & Orlin, J. B. (1993). *Network flows: theory, algorithms, and applications*.

[45] IBM ILOG (2014). *Cplex optimization studio*. [online]. Available: http://www-03.ibm.com/software/products/en/ibmilogcpleoptistud, last accessed August 2014.

[46] RTE. (2011). *Le réseau de transport d'électricité 400kv*. [online]. Available: http://www.rte-france.com, last accessed November 2011.

[47] EDF. (2013). *En direct de nos centrales*. [online]. Available: http://france.edf.com/france-45634.html, last accessed Avril 2013.

[48] European Commission. (2001). "Analysis of Electricity Network Capacities and Identification of Congestion – Final Report," Available: http://europa.eu.int/comm/energy/en/elec_single_market/index_en.html

[49] Zhou, Q., & Bialek, J. W. (2005). "Approximate model of European interconnected system as a benchmark system to study effects of cross-border trades," *Power Systems, IEEE Transactions on*, 20(2), 782-788.

[50] Fang Y.-P. Pedroni N., Zio E. (2014). "Comparing network-centric and power flow models for the optimal allocation of link capacities in a cascade-resilient power transmission network," *System Journal, IEEE*, vol.PP, no.99, pp.1,12, doi: 10.1109/JSYST.2014.2352152.

[51] Consulting V. (2014). *PopulationMondiale.com - World population clock: suivez l'évolution de la population du Monde en direct!* [online]. Available: http://www.world-gazetteer.com, last accessed 9 Sep. 2014.

[52] Padberg, M., & Rinaldi, G. (1991). "A branch-and-cut algorithm for the resolution of large-scale symmetric traveling salesman problems," *SIAM review*, 33(1), 60-100.

Paper [6] Y.-P. Fang, N. Pedroni, E. Zio. "Resilience-based component importance measures for infrastructure network systems." Reliability, IEEE Transaction on, 2014, under review.

Resilience-based component importance measures for critical infrastructure network systems

Yi-Ping Fang, Nicola Pedroni, Enrico Zio, *Senior Member, IEEE*

Y.-P. Fang is with the Chair on Systems Science and the Energetic challenge, École Centrale Paris and Supélec, France (e-mail: yiping.fang@ecp.fr)

N. Pedroni is with the Chair on Systems Science and the Energetic challenge, École Centrale Paris and Supélec, France (e-mail: nicola.pedroni@ecp.fr)

E. Zio is with the Chair on Systems Science and the Energetic challenge, École Centrale Paris and Supélec, Paris, France and with the Department of Energy, Politecnico di Milano, Milan, Italy (e-mail: enrico.zio@ecp.fr, enrico.zio@supelec.fr, enrico.zio@polimi.it)

Abstract – **In this paper, we propose two metrics, i.e. the optimal repair time and the resilience reduction worth, to measure the criticality of the components of a network system from the perspective of their contribution to system resilience. Specifically, the two metrics quantify (i) the priority with which a failed component should be repaired and re-installed into the network, and (ii) the potential loss in the optimal system resilience due to a time delay in the recovery of a failed component, respectively. Given the stochastic nature of disruptive events on infrastructure networks, a Monte Carlo-based method is proposed to generate probability distributions of the two metrics for all the components of the network; then, a stochastic ranking approach based on the Copeland's pairwise aggregation is used to rank components importance. Numerical results are obtained for the IEEE 30 Bus test network and a comparison is made with three classical centrality measures.**

Index Terms – **Critical Infrastructure, system resilience, component importance measures, system recovery, stochastic ranking**

I. INTRODUCTION

Complexity of critical infrastructures (CIs), such as power grids, the Internet, transportation networks, and so forth, is increasing. Disruptive events, whether they are malevolent attacks, natural disasters, or human-caused accidents, can have significant impacts on these real world complex networks composed of numerous interconnected functional and structural elements.

Justifiably, then, critical infrastructure protection (CIP) has become a priority for all nations [1]. The focus has been traditionally placed on physical protection and asset hardening [2]-[5]. However, in recent years, lessons learned from some catastrophic accidents have pushed part of the focus on the concept of

"resilience" [6], [7]. The outcomes of the 2005 World Conference on Disaster Reduction (WCDR) witness the significance of introducing the term "resilience" into the disaster discourse, giving birth to a new culture of disaster response [8]. Consequently, government policy has also evolved to encourage efforts that would allow assets to continue operating at some level, or quickly return to full operation after the occurrence of disruptive events [9].

"Resilience" comes from the Latin word "resilio" that literary means "to leap back" and denotes a system attribute characterized by the ability to recover from challenges or disruptive events. The Merriam-Webster dictionary defines resilience as "the ability to recover from or adjust easily to misfortune or change." In this view, systems should not only be reliable, i.e. having an acceptably low failure probability, but also resilient, i.e. having the ability to optimally recover from disruptions of the nominal operating conditions [10], [11].

In this context, the present paper addresses the issue of quantifying the *importance* of components in contributing to the *resilience* of a critical infrastructure. Component importance measures (CIMs) have been thoroughly studied in the field of reliability theory and risk analysis. Various analytical and empirical CIMs have been proposed in the literature, e.g. Birnbaum [12], Fussell-Vesely [13], Reliability Achievement/Reduction Worth [14], [15], and their extensions [16]-[20]. CIMs have been shown valuable in establishing direction and prioritization of actions related to an upgrading effort (e.g., *reliability* improvement) in system design, or in suggesting the most efficient way to operate and maintain system status. However, none of the existing classical CIMs based on the reliability concept are directly applicable to the post-disaster phase, since there is no scope to exhibit reliability after the occurrence of system failure.

The role that a component plays in a network system has been measured by various so-called centrality measures, looking from the point of view of the complex interaction and communication flow in the network [21], [22]. Classical topological centrality measures are the degree centrality [23], [24], the closeness centrality [24]-[26], the betweenness centrality [24], and the information centrality [27]. They specifically rely on topological information to qualify the importance of a network component. Additionally, Freeman et al. [28] proposed a *flow betweenness* centrality measure based on the idea of maximum network flow; Newmann [29] suggested a *random walk betweenness* measure that counts essentially all paths between vertices and which makes no assumptions of optimality; Jenelius et al. [30] proposed several vulnerability-based importance measures for transportation networks; Hines and Blumsack [31] introduced an "electrical centrality" measure for electrical networks by taking into account the electrical topology of the network; Zio and Piccinelli [32] provided a randomized flow model-based centrality measure specifically for electrical networks; Zio and Sansavini [33] introduced component criticality measures from the cascade failure process point of view, for general network systems.

Nevertheless, none of these analyses takes into account the dynamics of system recovery from the effects of a disruptive event.

Resilience-based metrics of component criticality with respect to their influence on the overall resilience of the system (i.e., on the system's ability to quickly recover from a disruptive event) can be helpful for preparing an efficient component repair checklist in the event of system failure [34]. Recently, Baker et al. [35] introduced two resilience-based network component importance metrics. However, the resilience definition, which the importance metrics rely on, does not embrace the temporal dimension of system recovery and it is, thus, unable to measure how fast the performance of a system comes back to an acceptable level. Besides, the two metrics do not quantify the influence that the recovery of particular components has on the overall resilience of the system and they are, thus, limited in providing valuable information for system restoration strategy making.

In this study, based on the definition of system resilience proposed in [36], we introduce two network components importance measures, namely, the optimal repair time and the resilience reduction worth, useful for prioritizing restoration activities. The two measures quantify (i) the priority with which a failed component should be repaired and re-installed into the network and (ii) the potential loss in the optimal system resilience due to a time delay in the recovery of a failed component, respectively. Both measures rely on the resilience optimization framework previously presented in [36]. A stochastic ranking technique, based on the Copeland's pairwise aggregation [37], is introduced to rank the components criticalities.

As a case study, the IEEE 30 Bus test network is considered: the criticalities of the components computed by the proposed indicators are compared to those produced by three classical measures of betweenness centrality [28], [29], [38].

The remainder of the paper is organized as follows. Section II provides the general framework of the study, recalling the definition of system resilience and the resilience optimization model originally proposed in [36]. In Section III, two measures of component criticality for system resilience, and a simulation methodology for their calculation and ordering are presented. Section IV illustrates the calculation of the proposed metrics on the IEEE 30 Bus test network: the obtained components rankings are compared to those produced by classical betweenness centrality measures. Concluding remarks are drawn in Section V.

II. METHODOLOGICAL BACKGROUND: SYSTEM RESILIENCE DEFINITION AND OPTIMIZATION FOR INFRASTRUCTURE NETWORK SYSTEMS

This section provides the definition of system resilience and the resilience optimization framework originally proposed in [36], which serve as methodological background for the resilience-based component importance measures that will be discussed in Section 3.

A. System Resilience Definition

As illustrated in Fig. 1, a quantifiable and time-dependent system performance function (also called system level delivery function or figure-of-merit) $F(t)$ is the basis for the assessment of system resilience. It has a nominal value $F(t_0)$ under nominal operating conditions. The system operates at this level until suffering a disruptive event at time t_e. The disruption generally deteriorates system performance to some level $F(t_d)$ at time t_d. Then, recovery action is started, affecting and improving system performance until it achieves, at a later time t_r, a targeted level of performance $F(t_r)$ that could be the same, close to, or better than original system performance $F(t_0)$), for which recovery is considered completed. The dotted curve $TF(t)$ in Fig. 1 denotes the targeted system performance if not affected by disruption, which is generally evolving due to the dynamic nature of service demand in the infrastructure system (in this study, it is assumed to be equal to $F(t_0)$ and remain invariant for simplicity). Besides, it is noted that various strategies exist for recovery activities, and system performance is ultimately a function of recovery decisions. The period of $t_d \leq t \leq t_r$ is generally considered as the recovery time [8].

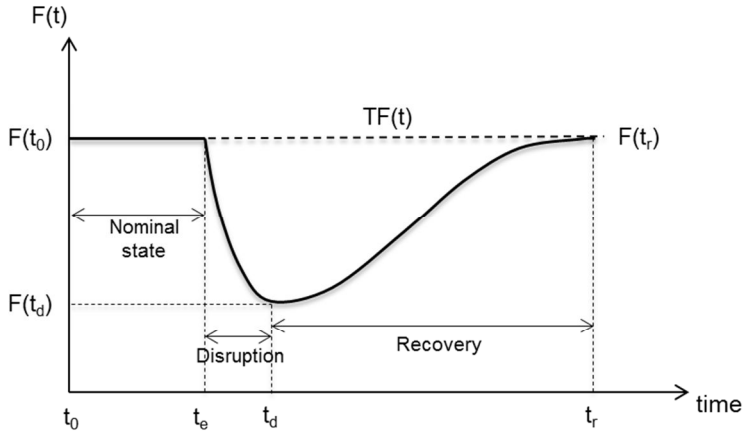


Fig. 1. Generic system performance transition curve under the occurrence of disruption.

Let $R(t)$ be the resilience of a system at time t ($t \geq t_d$). In its basic form, $R(t)$ describes the cumulative system functionality that has been restored at time t, normalized by the expected cumulative system functionality supposing that the system has not been affected by disruption during this time period (Eq. (1) below): graphically, $R(t)$ is quantified by the ratio of the area with diagonal stripes S_1 to the area of the shaded part S_2, as shown in Fig. 2.

$$R(t) = \frac{\int_{t_d}^{t}[F(\tau)-F(t_d)]d\tau}{\int_{t_d}^{t}[TF(\tau)-F(t_d)]d\tau}, t \geq t_d \quad (1)$$

Note that the formulation in Eq. (1) focuses mainly on the recoverability dimension of resilience and $R(t)$ is in the range of $[0, 1]$. $R(t) = 0$ when $F(t) = F(t_d)$, which means that a system has not recovered from its disrupted state (i.e., there has been no "resilience" action); $R(t) = 1$ when $F(t) = TF(t)$, which corresponds to the ideal case where a system recovers to its target state immediately after disruption. This resilience quantification is consistent with the original meaning of the concept of resilience and is capable of measuring at the same time the magnitude and rapidity of system recovery action.

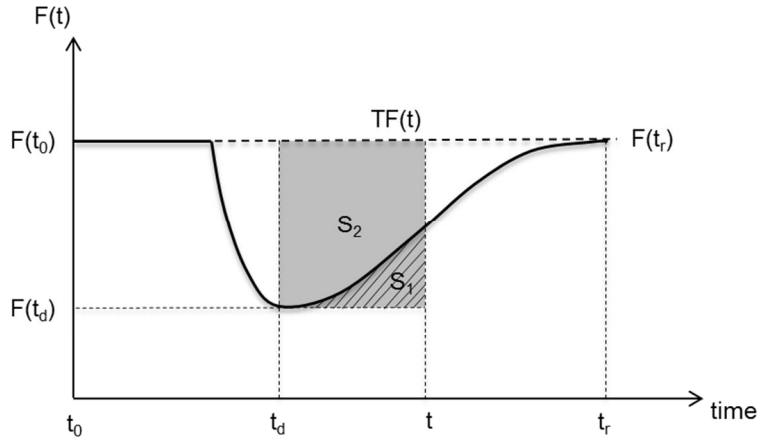


Fig. 2. Conceptual illustration of the proposed resilience measurement.

B. System Resilience Optimization

A disruptive event could impact one or more components of an infrastructure network system. In the case of multiple component failures, a systemic recovery action should be undertaken with the order of failed components to repair such that system resilience is maximal, i.e., to achieve optimal (restored) cumulative system functionality over the recovery time considered.

A variety of frameworks of optimization for post-disaster recovery of an infrastructure network system can be designed, focusing on different aspects of the restoration strategy, e.g., the order of repair of the damaged components, where and how to allocate repair resources and so forth. This study focuses on the significance of the recovery of a component with respect to the resilience of the system. Consequently, the optimization is designed to find the optimal order of repair of the set of failed components with the objective of achieving maximum system resilience over the restoration time horizon [36].

The mathematical model for the resilience optimization concerns a network $G(V, E)$ comprising a set of nodes V connected by a set of links or arcs E. The network nodes are distinguished in supply nodes V_S, transshipment nodes V_T and demand nodes V_D ($V_S \cup V_T \cup V_D = V$). Each arc $ij \in V$ has an associated

capacity $(ij) \in \boldsymbol{R}_0^+$, each supply node $i \in V_S$ has a supply capacity per time unit $P_i^s \in \boldsymbol{R}_0^+$ and each demand node $j \in V_D$ has a demand $P_j^D \in \boldsymbol{R}_0^+$ per time unit. Network flow is delivered from supply nodes to demand nodes respecting the flow capacities of the links and supply/demand capacities of the nodes. The performance of the network is evaluated by determining the maximum amount of flow that can be received by the demand nodes. Formally, the system performance function is defined as:

$$F(t) = \sum_{j \in V_D} f_j(t) \tag{2}$$

where $f_j(t)$ represents the amount of flow received by demand node j at time t.

Disruptions happen and create damages to nodes and/or links in the network, which is modeled as removal of a subset of arcs, $E' \subset E$, from the network.[1] The arcs in set E' are viewed as non-operational immediately after the disruption. System performance $F(t)$ achieves its minimum value at this time ($t = 0$, i.e. $F_{min} = F(0)$).

The recovery optimization framework aims at identifying the subset of links in E' to repair and the order, in which the links should be repaired so as to achieve maximum system resilience over the restoration horizon $T \in \boldsymbol{Z}^+$. Link repairs are assumed to be discrete tasks, and only a single arc can be repaired at any given timeslot. The repair time of arc restoration is not considered in this study (i.e., the repair action is assumed to be instantaneous); rather, the focus is on when the disrupted arcs should be brought back online. By combining Eqs. (1) and (2), system resilience to be maximized at time T is given by

$$R(T) = \frac{\sum_{t=1}^{t=T}\left[\sum_{j \in V_D} f_j(t) - F_{min}\right]}{T \cdot \left(\sum_{j \in V_D} P_j^D - F_{min}\right)} \tag{3}$$

The variables of the resilience optimization problem include: (i) continuous variables $f_{ij}(t) \in \boldsymbol{R}_0^+$, $ij \in E$ and $t = 1, \ldots, T$, that denote the flow moving from node i to node j through link ij at time unit t; (ii) continuous variables $f_j(t) \in \boldsymbol{R}_0^+$, $j \in V_D$, that represent the amount of flow received by demand node j at time unit t and (iii) binary state variables $s_{ij}(t)$, $ij \in E$ and $t = 1, \ldots, T$, such that $s_{ij}(t) = 1$ if arc ij is operational and $s_{ij}(t) = 0$ if arc ij is not operational at time unit t. We are interested in optimizing the resilience over the whole restoration process: thus, the timespan T is chosen as the total recovery time, defined as the period necessary to restore the system functionality to the same level as the original system. Consequently, the formulation of the resilience optimization problem is as follows:

$$\max \quad \frac{\sum_{t=1}^{t=T}\left[\sum_{j \in V_D} f_j(t) - F_{min}\right]}{T \cdot \left(\sum_{j \in V_D} P_j^D - F_{min}\right)} \tag{4}$$

Subject to

[1] For nodes, they can be converted to equivalent arcs by introducing additional arcs and nodes into the network, i.e. by 'splitting' a node into two nodes and an arc.

$$\sum_{(i,j)\in E} f_{ij}(t) - \sum_{(j,i)\in E} f_{ji}(t) \le P_i^s \qquad \forall i \in V_S, t = \{1, \dots, T\} \tag{5}$$

$$\sum_{(i,j)\in E} f_{ij}(t) - \sum_{(j,i)\in E} f_{ji}(t) = 0 \qquad \forall i \in V_T, t = \{1, \dots, T\} \tag{6}$$

$$\sum_{(i,j)\in E} f_{ij}(t) - \sum_{(j,i)\in E} f_{ji}(t) = -f_j(t) \quad \forall i \in V_D, t = \{1, \dots, T\} \tag{7}$$

$$0 \le f_j(t) \le P_j^D \qquad \forall i \in V_D, t = \{1, \dots, T\} \tag{8}$$

$$0 \le f_{ij}(t) \le s_{ij}(t)P(ij) \qquad \forall ij \in E, t = \{1, \dots, T\} \tag{9}$$

$$s_{ij}(t) \le s_{ij}(t+1) \qquad \forall ij \in E, t = \{1, \dots, T\} \tag{10}$$

$$\sum_{(i,j)\in E'} \left[s_{ij}(t) - s_{ij}(t-1)\right] = 1 \quad \forall t = \{1, \dots, T\} \tag{11}$$

$$s_{ij}(t) \in \{0,1\}, s_{ij}(0) = 0 \qquad \forall ij \in E, t = \{1, \dots, T\} \tag{12}$$

The objective (4) is to maximize the system resilience over the time horizon of recovery. Constraints (5)-(9) are typical network flow constraints over the links and supply/demand nodes in the network in period t. They ensure that: the flow generated at a supply node does not exceed its supply capacity (5); the amount of net injected flow at a transshipment node is zero (6); the amount of net injected flow at a demand node is equal to the received flow at the node (7) while not exceeding its requested demand (8); the flow on an operational link does not exceed its capacity and there is no flow passing through an arc if the arc is failed (9). Constraint (10) ensures that once an arc has been restored at time t, it will keep operational thereafter. Finally, constraint (11) ensures that only a single arc can be repaired at any given timeslot.

This resilience optimization above defined is a typical mixed integer programming (MIP) problem. A commercial optimization solver Cplex [39] is used in this study for its solution. It is noted that this resilience optimization model is only applied for the purpose of illustration of resilience-based component importance metrics. More complex optimization models (e.g., taking into account the cost and duration of repairing a particular failed link) can be adopted in other application cases.

III. Resilience-Based Component Importance Measures For Infrastructure Network Systems

A. Component Importance Measures Definition

As described in Section 2.2, the analysis concerns a network $G(V, E)$ comprising a set of nodes V and a set of links E. The binary state variable of arc ij at time t is defined by $s_{ij}(t)$, $\forall ij \in E$. The initial impact experienced by the network after a disruptive event e at time $t = 0$ is represented by the removal of a subset of arcs, $E' \subset E$, from the network, setting $s_{ij}(0) = 0, \forall ij \in E'$. We introduce the failure probability of arc ij under event e, $p_e(ij)$

$$P\left[s_{ij}(0) = 0 | e\right] = p_e(ij), \forall ij \in E \tag{13}$$

Eq. (13) describes how individual components (links) are initially affected by a disruptive event e; Section 2.2 explains how these failed components optimally recover from the disruption state following the event; finally, Eq. (1) incorporates these dimensions to quantify system resilience.

When considering component criticality in a resilience setting, we are interested in understanding: (i) the optimal time to repair the failed components in order to maximize system resilience, and (ii) the effect that the timely recovery of the components have on the overall resilience of the system. These concepts are at the basis of the definition of the two resilience-based importance measures here proposed.

Given a particular initial failure state, the optimal repair time T_{ij}^{opt} of a failed arc ij can be computed by solving the MIP problem (4) - (12):

$$T_{ij}^{opt} = arg\ \max_{T_{ij} \in [0,T]} R(T) \tag{14}$$

The timespan for restoration, T, is chosen as the time period necessary to restore the system functionality to the same level as the original system. It is noted that the optimal repair time T_{ij}^{opt} offers an explicit quantification of the priority that should be given to the reparation and installation of arc ij into the network. Low values of T_{ij}^{opt} indicate higher priority of being repaired and re-installed into the network, i.e. higher ranking of the component in the repair checklist.

To account for the delay in the restoration of a particular link ij, a resilience reduction worth (RRW) metric is introduced as

$$RRW_{ij}(\Delta t_0) = \frac{R^{opt}(T) - R^{opt}(T|T_{ij} \geq T_{ij}^{opt} + \Delta t_0)}{R^{opt}(T)} \tag{15}$$

where $R^{opt}(T)$ represents the optimal system resilience at restoration time T; $R^{opt}(T|T_{ij} \geq T_{ij}^{opt} + \Delta t_0)$ corresponds to the optimal system resilience at time T if link ij cannot be repaired until time $(T_{ij}^{opt} + \Delta t_0)$, where Δt_0 is the delay with respect to its optimal repair time T_{ij}^{opt}, Eq. (14). Eq. (15) quantifies the potential (normalized) loss in optimal system resilience due to a delay Δt_0 in the repair of link ij. This metric is comparable to the so-called reliability reduction worth [40], which measures the potential damage caused to the system reliability by the failure of a particular component. It can provide valuable information to guide the recovery process of a particular component. Components with high values of $RRW_{ij}(\Delta t)$ should be given high priority in the restoration process, e.g. be assigned adequate restoration resources to avoid delays that would have a more significant impact on system restoration.

B. Methodology for Component Importance Ordering

Ordering network links recovery on the basis of the values of the criticality measures described above, i.e., the optimal repair time T_{ij}^{opt} and resilience reduction worth RRW_{ij} (fixed Δt_0), requires quantifying the effect of timely repairing these links on the overall resilience of the system. Given the stochastic nature of disruptive events in terms of components failures after the event, the resilience-based criticality measures introduced are not represented by deterministic values, but rather by probability distributions. Therefore, given a network $G(V, E)$ under a disruptive event e, we first apply a Monte Carlo-based method to

generate distributions of optimal repair time T_{ij}^{opt} and resilience reduction worth $RRW_{ij}(\Delta t_0)$ for all the links in the network; then, we rank links importance using a stochastic approach based on the Copeland's pairwise aggregation method [37]. The detailed steps of the algorithm are as follows:

Step 1. A network $G(V, E)$ is initially operating with a given parameters setting: flow demand P_j^D of all the demand nodes in V_D, supply capacity P_i^S of all the supply nodes in V_S and link capacity $P(ij)$ for all the network arcs in E.

Step 2. A failure configuration of the network is randomly sampled on the basis of the failure probabilities of each arc in the system given by Eq. (13), under a disruptive event e at initial time $t = 0$. The operation state variables of failed links are set to 0, i.e., $s_{ij}(0) = 0, \forall ij \in E'$.

Step 3. The resilience optimization model of Eq. (4) - (12) is applied and solved by Cplex to obtain the optimal strategy of network recovery, i.e., the optimal repair time T_{ij}^{opt} for each failed arc $ij \in E'$.

Step 4. In order to evaluate the second importance measure $RRW_{ij}(\Delta t_0)$, for each failed arc $ij \in E'$, the additional constraint that the restoration of arc ij should not be accomplished earlier than $T_{ij}^{opt} + \Delta t_0$ (i.e., $T_{ij} \geq T_{ij}^{opt} + \Delta t_0$) is added to the optimization model of Eq. (4) – (12). Then, $R^{opt}(T|T_{ij} \geq T_{ij}^{opt} + \Delta t_0)$ is obtained by solving this "modified" optimization model by Cplex. Finally, the resilience reduction worth $RRW_{ij}(\Delta t_0)$ for each arc ij is recorded.

Step 5. To account for the stochasticity of the disruptive event in terms of arcs failures, repeat Step 2 to Step 4 for a chosen number $\aleph$ of iterations, generating probability distributions for T_{ij}^{opt} and $RRW_{ij}(\Delta t_0)$, for all the links in the network.

Step 6. Given the distributions of T_{ij}^{opt} (resp., $RRW_{ij}(\Delta t_0)$) for each arc ij, perform a stochastic ranking of links according to ascending (resp., descending) T_{ij}^{opt} values (see Section III.*B*.1).

1) Stochastic Ranking

In order to rank network links according to the distribution of their optimal repair time T_{ij}^{opt} (or resilience reduction worth $RRW_{ij}(\Delta t_0)$) obtained at step 6 of the algorithm above, an approach based on the Copeland's pairwise aggregation method [37] is proposed. The Copeland's method (CM) is a simple non-parametric Condorcet method used in the political field (voting) that does not require any information about decision maker preference and operates on a multi-indicator matrix formed by m objects characterized by Ω attributes [41]. CM relies on pair-wise comparisons between objects in the candidate pool, and the so-called Copeland score is defined for each object as the difference between the number of times that this object beats the other objects and the number of times that it is beat by other objects.

The CM-based ranking approach applied here corresponds to a modification proposed by Al-Sharrah [42]. It first examines the CDF of a given variable for all the candidates, e.g., the CDF of $T_{ij}^{opt}, \forall (i, j) \in E$; then, it

compares the CDF of two candidates under analysis, i.e., links ij and $\overline{ij}$, with respect to specific attributes q_k of the CDF: for example, attribute q_k may represent the kth percentile. Subsequently, a quantity $S_k(ij, \overline{ij})$ is calculated based on a pairwise comparison between links ij and $\overline{ij}$ with respect to (percentile) q_k of the corresponding distributions, $k = 1, \dots, \Omega$:

$$S_k(ij, \overline{ij}) \begin{cases} C_{k-1}(ij, \overline{ij}) + 1, & \text{if } q_k(ij) \text{ beats } q_k(\overline{ij}) \\ C_{k-1}(ij, \overline{ij}) + 0.5, & \text{if } q_k(ij) \text{ and } q_k(\overline{ij}) \text{ are tied} \\ C_{k-1}(ij, \overline{ij}), & \text{if } q_k(ij) \text{ beats } q_k(\overline{ij}) \end{cases} \tag{16}$$

where the sentence "$q_k(ij)$ beats $q_k(\overline{ij})$" means that $q_k(ij)$ dominates $q_k(\overline{ij})$ with respect to the ranking rule of the variable considered, i.e., $q_k(ij) < q_k(\overline{ij})$ for T_{ij}^{opt}, while $q_k(ij) > q_k(\overline{ij})$ if $RRW_{ij}(\Delta t_0)$ is considered. $S_0(ij, \overline{ij})$ is initialized at zero for the first (percentile) q_1 and Eq. (16) is iterated through all Ω attributes (percentiles). Then, the Copeland score for each link ij is defined as

$$C(ij) = \sum_{\overline{ij} \neq ij} S_\Omega(ij, \overline{ij}) \tag{17}$$

This Copeland score is finally used to rank all the links: the higher $C(ij)$, the higher the contribution of link ij to the overall resilience of the network.

IV. CASE STUDY

A. Resilience-Based Criticality Measures on The IEEE 30 Bus Test System

The IEEE 30 Bus test system [43] is taken as reference case study for the proposed resilience-based component importance measure approach. This system (Fig. 3) represents a portion of the American Electric Power System and is composed of 30 buses connected by 41 transmission lines. To carry out the analysis, each system component is transposed into a node or edge of the representative topological network, as it is shown in Fig. 4. Three different physical types of nodes are considered: generator nodes (where the electricity flow is fed into the network), demand nodes (where customers are connected) and transfer or transmission nodes (without customers or sources).

The simulation procedure introduced in Section 3.2 is, then, used to rank each component of the IEEE 30 Bus network according to the criticality metrics introduced. In normal conditions, the network is assumed to operate under the following parameters setting: the generation capacity is identical for all generation nodes and equal to 60, in arbitrary units (a.u.); the flow demands are 20 a.u. for all load nodes; the values of the transmission capacities are 20 a.u. for all the network links. The homogeneous assignments of generation capacity, demand and link capacity are here applied for the purpose of identifying the resilience criticalities of all the network arcs stemming from their different topological connections. For the same reason, a constant failure probability $p_e(ij)$ is assumed for all the network links under disruptive

event e. The roulette wheel selection method [44] is used in step 2 for sampling a failure configuration by selecting a failed link at each spin until a certain number $\|E\| \cdot p_e(ij) = 12$ of arcs are selected.

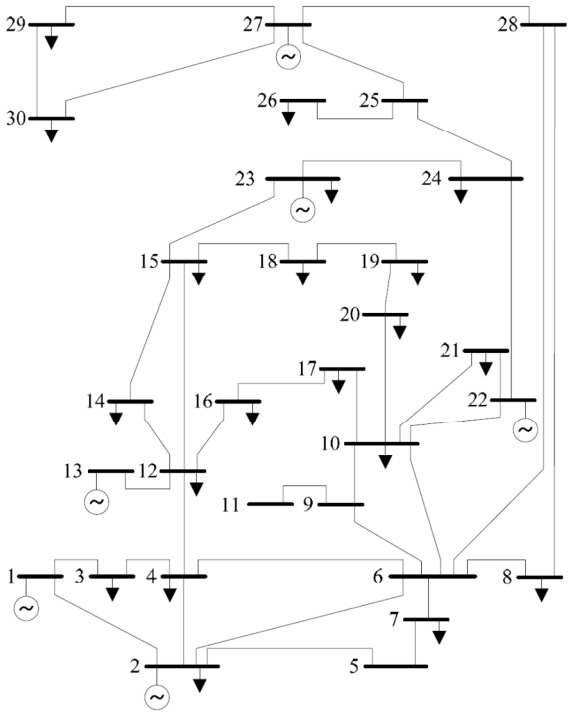


Fig. 3. Single line diagram of the IEEE 30 Bus test system.

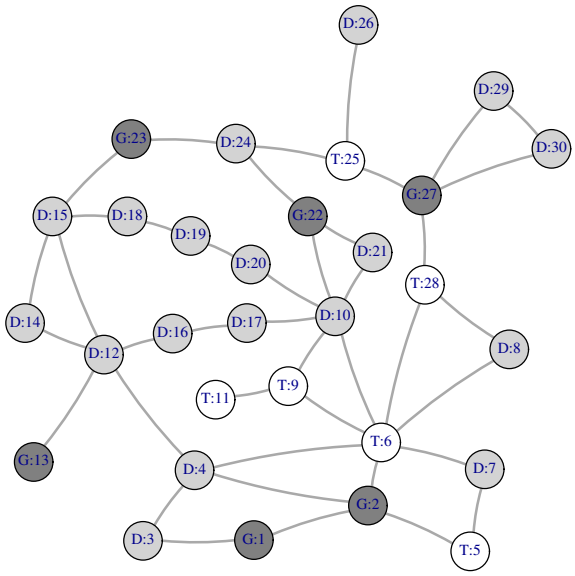


Fig. 4. Graph representation of the IEEE 30 Bus test system. The dark grey circles labeled with G represent the generator nodes, the white circles labeled with T represent transmission nodes and the light grey circles labeled with D represent the demand nodes.

Fig. 5 illustrates the Cumulative Distribution Functions (CDFs) of T_{ij}^{opt} for five representative links (<1, 3>, <5, 7>, <27, 30>, <8, 28> and <10, 21>), obtained at step 5 of the procedure by applying the simulation algorithm proposed in Section 3.2 (for $\aleph = 1000$ samples). The Figure illustrates the probability that T_{ij}^{opt} is less than or equal to a target value x. It can be seen that the optimal repair time associated with link <1, 3>, i.e. T_{13}^{opt}, will never be larger than 5 (square-line curve in Fig. 5). Moreover, the curve for link <1, 3> always "dominates" the other curves. Therefore, this link should have the highest priority to be repaired in order to maximize system resilience.

However, considering e.g. links <5, 7> (circle line) and <27, 30> (triangle line) in Fig. 5, it is not evident which one "dominates" the other, due to the intersection of their CDF curves. Thus, the CM-based ranking approach introduced in Section 3.2.1 is applied to rank the importance of the links. Fig. 6 reports the Copeland scores of all the 41 links in the IEEE 30 Bus network, ordered in descending order, with link <1, 3> having the highest score, followed by links <2, 6>, <2, 4>, <10, 22> and so forth. Furthermore, Fig. 7 graphically illustrates the Copeland score of the optimal repair time T_{ij}^{opt} for all IEEE 30 Bus network links, where links with higher values of Copeland score are represented as thicker and darker edges. It is shown that two types of links are more important in terms of T_{ij}^{opt}: i) the links which connect the generator nodes with the other two types of nodes (transmission nodes and demand nodes), e.g. links <2, 6>, <1, 3>, <12, 13> etc., and ii) the links which are the only ones connected to demand nodes, e.g. link <25, 26>. The restoration of these types of links is most likely able to augment the total amount of flow received by the demand nodes of the network: thus, high priority should be given to these links when considering the repair order of the failed links.

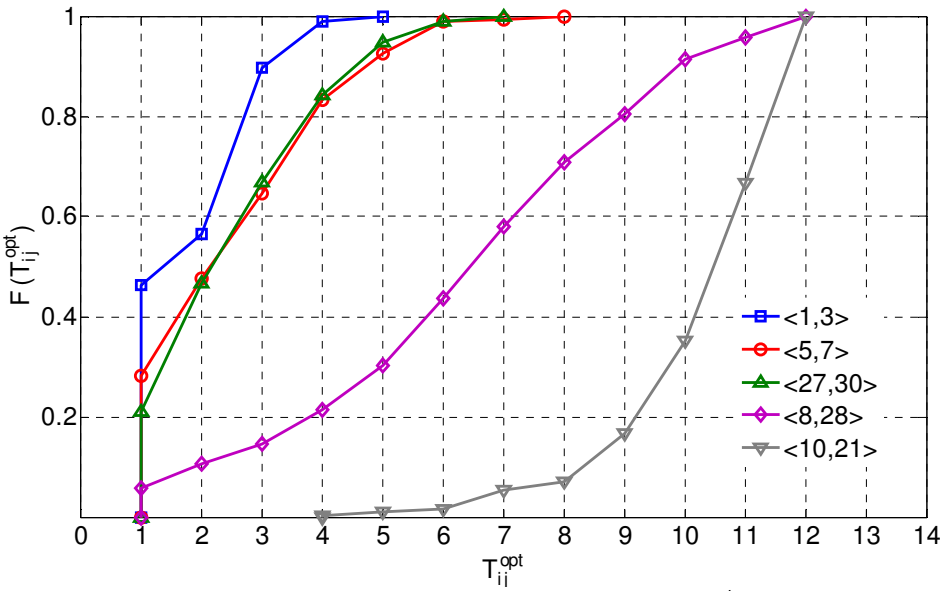


Fig. 5. Cumulative probability distributions of the optimal repair time T_{ij}^{opt} for five representative links.

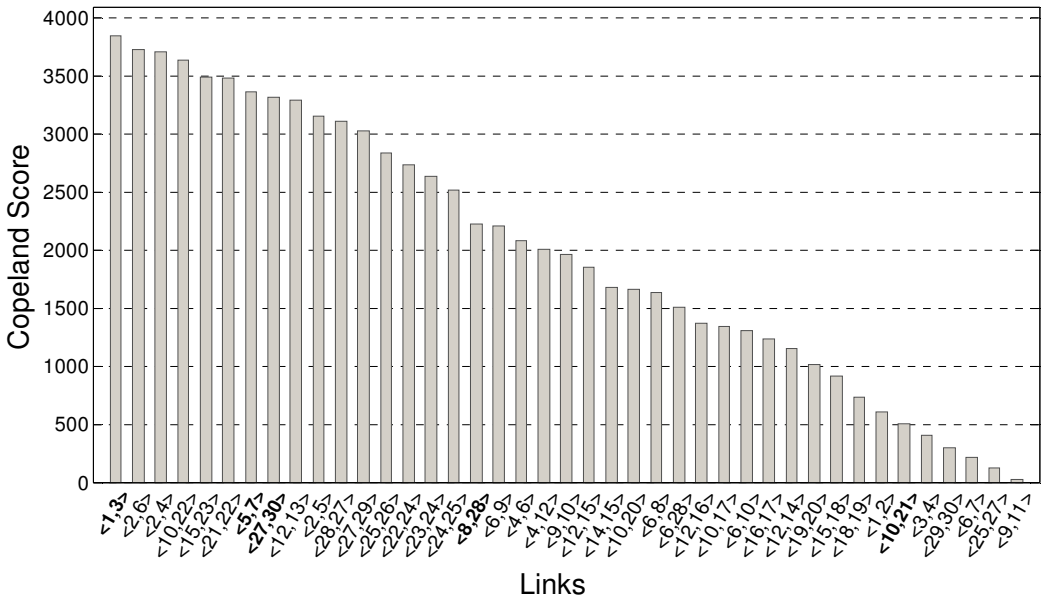


Fig. 6. Copeland score ranking of the optimal repair time T_{ij}^{opt} for all IEEE 30 Bus network links.

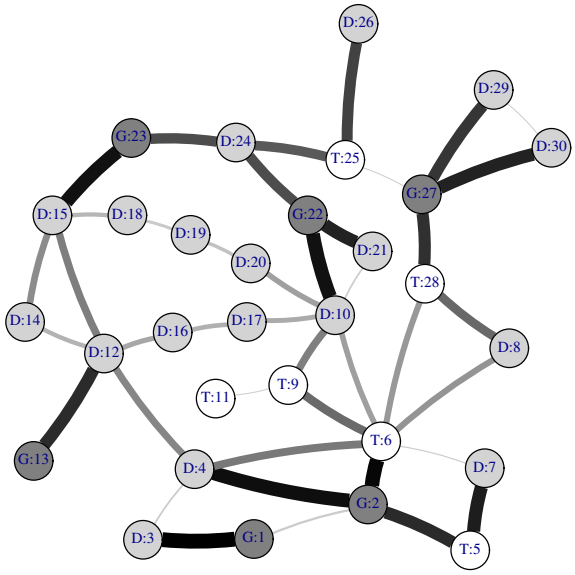


Fig. 7. Graphical illustration of the Copeland scores of the optimal repair time T_{ij}^{opt} for all IEEE 30 Bus network links. Links with higher value of Copeland score are represented as thicker and darker edges.

Fig. 8 and Fig. 9 illustrate the results based on the resilience reduction worth $RRW_{ij}(\Delta t_0)$ for all the links and for a delay time $\Delta t_0 = 3$ units (i.e., the Copeland score ranking and its graphical representation, respectively). It is shown that <24, 25> is the most critical link in terms of RRW_{ij}, i.e. a delay in its restoration would cause the largest reduction in system resilience among all the network links; thus, adequate resources should be given to make sure of its timely restoration. Besides, it is noted that the links with high Copeland scores in terms of the optimal repair time T_{ij}^{opt} also have high Copeland score ranking

in terms of the resilience reduction worth RRW_{ij}: the correlation coefficient between the two Copeland scores is $r\left(C_{T_{ij}^{opt}}, C_{RRW_{ij}}\right) = 0.82$ for $\Delta t_0 = 3$.

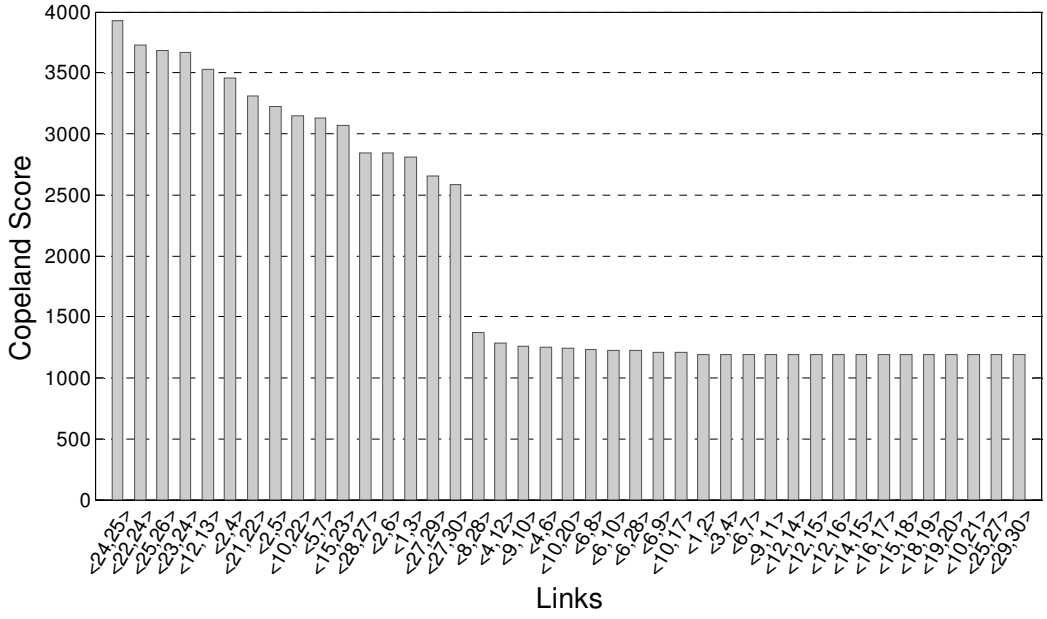


Fig. 8. Copeland score ranking of the resilience reduction worth $RRW_{ij}(\Delta t_0 = 3)$ for all IEEE 30 Bus network links.

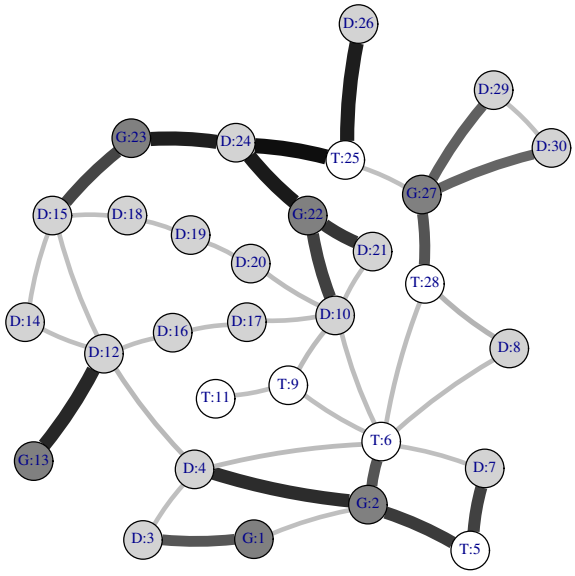


Fig. 9. Graphical illustration of the Copeland scores of the resilience reduction worth $RRW_{ij}(\Delta t_0 = 3)$ for all IEEE 30 Bus network links. Links with higher values of Copeland score are represented as thicker and darker edges.

B. Comparison with Betweenness Centrality Measures

Betweenness centrality indices have been introduced as measures of component importance in a network, taking into account the different ways in which a component interacts and communicates with the rest of the network [24], [32]. A classical centrality measure is the topological betweenness centrality introduced in the social network field, which is based on the idea that a component is central if it is lies between many other components, in the sense that it is traversed by many of the shortest paths connecting pairs of nodes [24], usually called as *shortest path betweenness*. The topological betweenness centrality C_{ij}^{B} of a given link ij in a supply-demand-differentiated network $G(V_S \cup V_T \cup V_D, E)$ is given by [38]:

$$C_{ij}^{B} = \frac{1}{\|V_S\| \cdot \|V_D\|} \sum_{s \in V_S, d \in V_D} \frac{n_{sd}(ij)}{n_{sd}}, ij \in E \tag{18}$$

where n_{sd} is the number of topological shortest paths between supply nodes and demand nodes, and $n_{sd}(ij)$ is the number of supply-demand shortest paths passing though link ij.

To account for the issue that in some cases flow may not follow the ideal geodesic paths from supply to demand nodes, a betweenness centrality measure based on the idea of maximum network flow has been proposed [28], usually known as *flow betweenness*. The measure counts all independent paths that carry information when a maximum flow is pumped between each pair of vertices. The flow betweenness of a component is defined as the amount of flow through it when the maximum flow is transmitted from source s to demand d, averaged over all s and d. It is quantitatively defined as [28]

$$C_{ij}^{F} = \frac{\sum_{s \in V_S, d \in V_D} m_{sd}(ij)}{\sum_{s \in V_S, d \in V_D} m_{sd}}, ij \in E \tag{19}$$

where m_{sd} is the maximum flow from a source node s to a demand node d and $m_{sd}(ij)$ is the maximum flow from s to d that passes through link ij.

In practical terms, however, neither of the two betweenness measures introduced above is realistic. Both count only a small subset of possible paths between vertices, and both assume some kind of optimality in information transmission (shortest paths or maximum flow). Therefore, a new betweenness measure that counts essentially all paths between vertices and which makes no assumptions of optimality has been suggested, called *random walk betweenness* [29]. This measure is based on random walks between vertex pairs and asks, in essence, how often a given component will fall on a random walk between another pair of vertices. Roughly speaking, the random walk betweenness of a link ij is equal to the number of times that a random walk starting at s and ending at d passes through the link along the way, averaged over all s and d. Let I_{ij}^{sd} be the current flow from s to d, through link ij. Then, the random walk betweenness of a link ij is defined as

$$C_{ij}^{RW} = \frac{1}{\|V_S\| \cdot \|V_D\|} \sum_{s \in V_S, d \in V_D} I_{ij}^{sd}, ij \in E \tag{20}$$

We are interested in comparing the ranking results of our resilience-based component importance measures to these betweenness centrality indices, i.e., *shortest path betweenness*, *flow betweenness* and *random walk betweenness* for the proposed IEEE 30 Bus network. Fig. 10 shows the values of the Copeland scores for the optimal repair time $C_{T_{ij}^{opt}}$ (left panel) and for the resilience reduction worth $C_{RRW_{ij}}$ (right panel) plotted with respect to the *shortest path betweenness* C_{ij}^{B} for all the links of IEEE 30 Bus network. No obvious correlation can be identified from the figures. Actually, the correlation coefficients between $C_{T_{ij}^{opt}}$, $C_{RRW_{ij}}$ and C_{ij}^{B} are $r\left(C_{T_{ij}^{opt}}, C_{ij}^{B}\right) = 0.08$ and $r\left(C_{RRW_{ij}}, C_{ij}^{B}\right) = 0.14$, respectively. Similarly, Fig. 11 plots the relationship between the Copeland scores for the optimal repair time $C_{T_{ij}^{opt}}$ (left panel) and the resilience reduction worth $C_{RRW_{ij}}$ (right panel) with the *flow betweenness* C_{ij}^{F}; Fig. 12 shows the same scatterplots with respect to the *random walk betweenness* C_{ij}^{RW}. The correlation coefficients are $r\left(C_{T_{ij}^{opt}}, C_{ij}^{F}\right) = 0.002$, $r\left(C_{RRW_{ij}}, C_{ij}^{F}\right) = -0.24$, $r\left(C_{T_{ij}^{opt}}, C_{ij}^{RW}\right) = 0.24$ and $r\left(C_{RRW_{ij}}, C_{ij}^{RW}\right) = 0.32$, respectively.

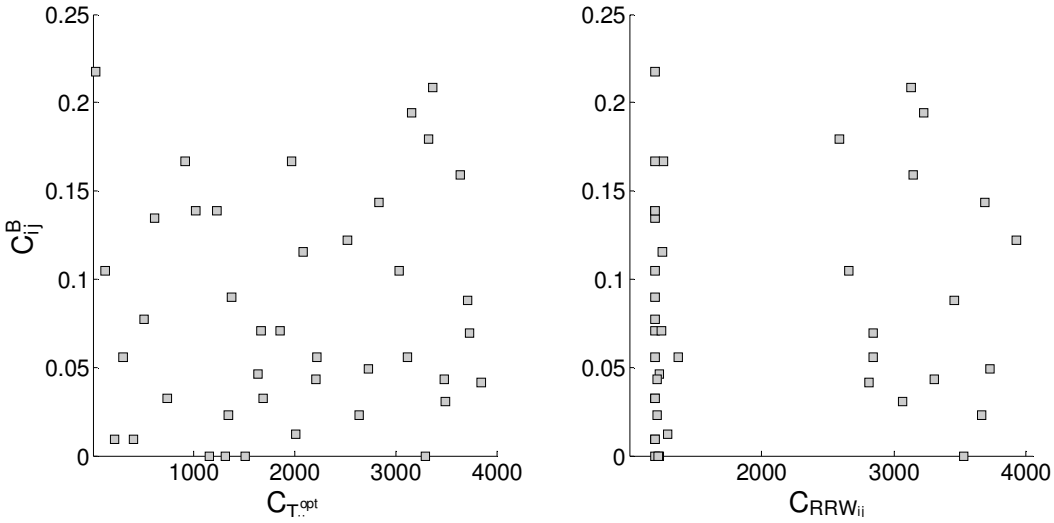


Fig. 10. Scatterplot of the Copeland scores of the optimal repair time $C_{T_{ij}^{opt}}$ (left panel) and resilience reduction worth $C_{RRW_{ij}}$ (right panel) with the shortest path betweenness C_{ij}^{B} for the links of the IEEE 30 Bus network.

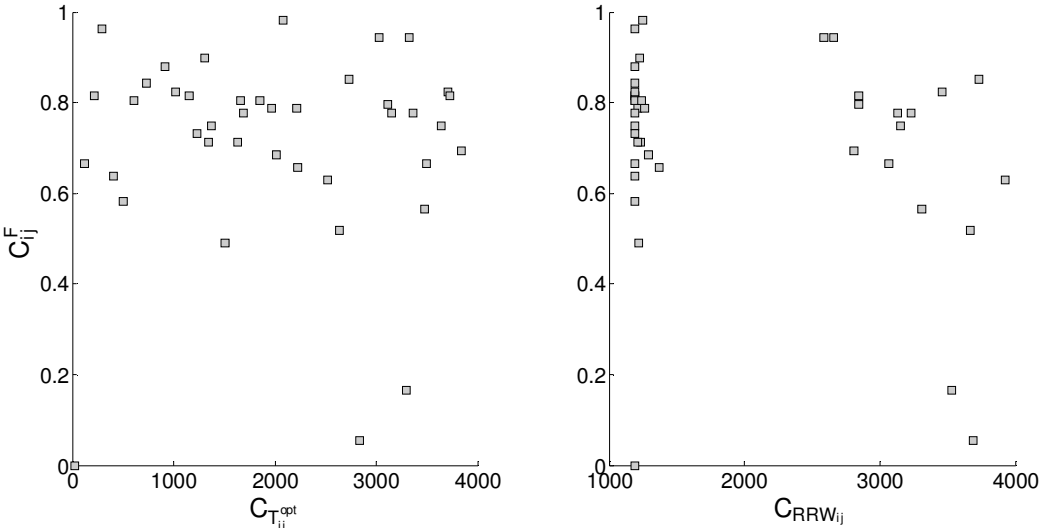


Fig. 11. Scatterplot of the Copeland scores of the optimal repair time $C_{T_{ij}^{opt}}$ (left panel) and resilience reduction worth $C_{RRW_{ij}}$ (right panel) with flow betweenness C_{ij}^{F} for the links of the IEEE 30 Bus network.

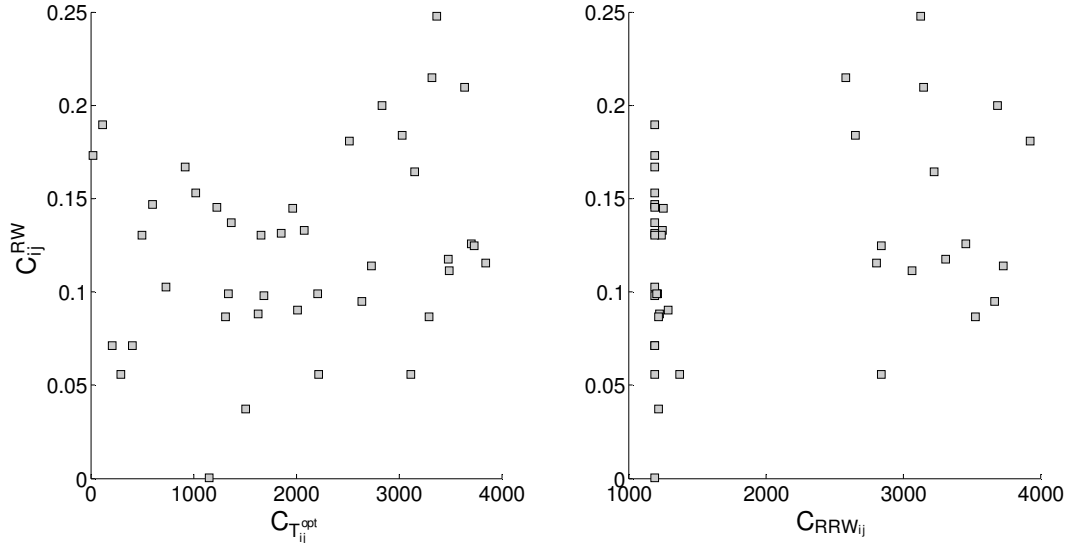


Fig. 12. Scatterplot of the Copeland scores of the optimal repair time $C_{T_{ij}^{opt}}$ (left panel) and resilience reduction worth $C_{RRW_{ij}}$ (right panel) with the random walk betweenness C_{ij}^{RW} for the links of the IEEE 30 Bus network.

These results show that the betweenness centrality indices (e.g., *shortest path betweenness*, *flow betweenness* and *random walk betweenness*) do not capture the component criticality with respect to resilience for the recovery of the IEEE 30 Bus network. This implies that these centrality measures (which are calculated under normal operation condition) are not applicable to guide the system restoration after a disruptive event, e.g., to prepare an efficient component repair priority checklist in the event of system failure.

V. CONCLUSIONS

This paper primarily contributes two metrics to measure the criticality of network components from the perspective of their contribution to system resilience, defined as the cumulative system functionality that has been restored at time t, normalized by the expected cumulative system functionality supposing that the system has not been affected by disruption during this time period.

The first resilience-based component importance measure, i.e. the optimal repair time T_{ij}^{opt} in Eq. (14), offers an explicit quantification of the priority that should be given to arc ij to be repaired and re-installed into the network. Lower values of T_{ij}^{opt} indicate higher priority, i.e. higher rank in the component repair checklist for system restoration in the event of system failure. The second resilience-based component importance measure, i.e. the resilience reduction worth $RRW_{ij}(\Delta t_0)$, quantifies the potential loss in optimal system resilience due to a delay Δt_0 in the repair time of link ij. This measure can provide valuable information to guide the recovery process of a particular component: components with high values of $RRW_{ij}(\Delta t_0)$ should be given high priority to their timely restoration, e.g. be assigned with adequate restoration resources.

Given the stochastic nature of disruptive events on an infrastructure network, a Monte Carlo-based method has been proposed to generate distributions of optimal repair time T_{ij}^{opt} and resilience reduction worth $RRW_{ij}(\Delta t_0)$ for all the components in the network; then, a stochastic ranking approach based on the Copeland's pairwise aggregation method has been applied to rank components importance.

The results of the two measures applied to the IEEE 30 Bus test network demonstrate some non-obvious and meaningful conclusions about the contributions of certain links to the resilience of the network. It is shown that two types of links are most important in terms of T_{ij}^{opt}: i) the links which connect generator nodes with the other two types of nodes (transmission nodes and demand nodes), e.g. links <2, 6>, <1, 3>, <12, 13> etc., and ii) the link which is the only arc connecting to demand nodes, i.e., link <25, 26>. The restoration of these types of links is most likely able to augment the total amount of flow received by the demand nodes of the network so that high priority should be given to these links in the reparation list. Besides, those links with high Copeland scores in terms of T_{ij}^{opt} also have high Copeland scores ranking in terms of the resilience reduction worth RRW_{ij}: actually, the correlation coefficient between the two quantities is $r\left(C_{T_{ij}^{opt}}, C_{RRW_{ij}(3)}\right) = 0.82$.

Finally, it is shown that the classical betweenness centrality indices, such as the *shortest path betweenness*, *flow betweenness* and *random walk betweenness*, do not capture resilience criticality as do the resilience-based measures T_{ij}^{opt} and $RRW_{ij}(\Delta t_0)$. In this view, the two measures newly proposed in this paper can provide precious insights to practical restoration activities for the components of infrastructure networks.

Future studies will concentrate on the application of the resilience-based component importance measures to larger and different types of infrastructure networks subject to realistic disruptive events in order to further demonstrate the practical effectiveness of the measures.

REFERENCE

[1] Zio, E. (2013). The Monte Carlo simulation method for system reliability and risk analysis. Springer.

[2] Lewis, T. G. (2006). Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.

[3] Clinton, W. (1998). "Presidential Decision Directive PDD-63, Protecting America's Critical Infrastructures," Washington, D.C.

[4] Bush, G.W. (2002). "Homeland Security Presidential Directive-3 (HSPD-3)," Washington, D.C.

[5] Bush, G.W. (2003). "Homeland Security Presidential Directive-7 (HSPD-7)," Washington, D.C.

[6] Pursiainen, C. (2009). The challenges for European critical infrastructure protection. European Integration, 31(6), 721-739.

[7] Obama, B. (2013). "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience," Washington, D.C.

[8] Cimellaro, G. P., Reinhorn, A. M., & Bruneau, M. (2010). Framework for analytical quantification of disaster resilience. Engineering Structures, 32(11), 3639-3649.

[9] Moteff, J. D. (2012). Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. Congressional Research Service.

[10] Zio, E. (2009). Reliability engineering: Old problems and new challenges. Reliability Engineering & System Safety, 94(2), 125-141.

[11] Zio. E. (2015). Challenges in the vulnerability and risk analysis of critical infrastructures: the need for an extended framework. Submitted to Reliability Engineering & System Safety.

[12] Birnbaum, Z.W. (1969). On the importance of different components in a multicomponent system. Multivariate Analysis 2, New York, Academic Press.

[13] Fussell, J. (1975). How to calculate system reliability and safety characteristics. IEEE Transactions on Reliability, 24(3), 169-174.

[14] Gandini, A. (1990). Importance and sensitivity analysis in assessing system reliability. IEEE Transactions on Reliability, 39(1), 61-70.

[15] Levitin, G., Podofillini, L. and Zio, E. (2003). Generalized importance measures for multistate elements based on performance level restrictions. Reliability Engineering and System Safety, 82, 63-73.

[16] Ramirez-Marquez, J. E., & Coit, D. W. (2005). Composite importance measures for multi-state systems with multi-state components. Reliability, IEEE Transactions on, 54(3), 517-529.

[17] Ramirez-Marquez, J. E., & Coit, D. W. (2007). Multi-state component criticality analysis for reliability improvement in multi-state systems. Reliability Engineering & System Safety, 92(12), 1608-1619.

[18] Andrews, J. D., & Beeson, S. (2003). Birnbaum's measure of component importance for noncoherent systems. Reliability, IEEE Transactions on, 52(2), 213-219.

[19] Wang, W., Loman, J., & Vassiliou, P. (2004). Reliability importance of components in a complex system. In Reliability and Maintainability, 2004 Annual Symposium-RAMS (pp. 6-11). IEEE.

[20] Fang Y.-P., & Zio E. (2013). Hierarchical Modeling by Recursive Unsupervised Spectral Clustering and Network Extended Importance Measures to Analyze the Reliability Characteristics of Complex Network Systems. American Journal of Operations Research, Vol. 3 No. 1A, 2013, pp. 101-112.

[21] Borgatti, S. P. (2005). Centrality and network flow. Social networks, 27(1), 55-71.

[22] Kröger, W., & Zio, E. (2011). Vulnerable systems. Springer, Berlin.

[23] Nieminen, J. (1974). On the centrality in a graph. Scandinavian Journal of Psychology, 15(1), 332-336.

[24] Freeman, L. C. (1979). Centrality in social networks conceptual clarification. Social networks, 1(3), 215-239.

[25] Sabidussi, G. (1966). The centrality index of a graph. Psychometrika, 31(4), 581-603.

[26] Wasserman, S., and Faust, K. (1994). Social Network Analysis: Methods and. Applications. Cambridge, ENG and New York: Cambridge University Press.

[27] Latora, V., & Marchiori, M. (2007). A measure of centrality based on network efficiency. New Journal of Physics, 9(6), 188.

[28] Freeman, L. C., Borgatti, S. P., & White, D. R. (1991). Centrality in valued graphs: A measure of betweenness based on network flow. Social networks, 13(2), 141-154.

[29] Newman, M. E. (2005). A measure of betweenness centrality based on random walks. Social networks, 27(1), 39-54.

[30] Jenelius, E., Petersen, T., & Mattsson, L. G. (2006). Importance and exposure in road network vulnerability analysis. Transportation Research Part A: Policy and Practice, 40(7), 537-560.

[31] Hines, P., & Blumsack, S. (2008, January). A centrality measure for electrical networks. In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual (pp. 185-185). IEEE.

[32] Zio, E., & Piccinelli, R. (2010). Randomized flow model and centrality measure for electrical power transmission network analysis. Reliability Engineering & System Safety, 95(4), 379-385.

[33] Zio, E., & Sansavini, G. (2011). Component criticality in failure cascade processes of network systems. Risk Analysis, 31(8), 1196-1210.

[34] Natvig, B., Huseby, A. B., & Reistadbakk, M. O. (2011). Measures of component importance in repairable multistate systems—a numerical study. Reliability Engineering & System Safety, 96(12), 1680-1690.

[35] Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2013). Resilience-based network component importance measures. Reliability Engineering & System Safety, 117, 89-97.

[36] Fang Y.-P., Pedroni N., & Zio E. (2014). Assessment and optimization of the resilience of infrastructure network systems subject to disruptive events. Submitted to System Journal, IEEE.

[37] Merlin, V. R., & Saari, D. G. (1997). Copeland method II: Manipulation, monotonicity, and paradoxes. Journal of Economic Theory, 72(1), 148-172.

[38] Kinney, R., Crucitti, P., Albert, R., & Latora, V. (2005). Modeling cascading failures in the North American power grid. The European Physical Journal B-Condensed Matter and Complex Systems, 46(1), 101-107.

[39] IBM ILOG (2014). Cplex optimization studio. http://www-03.ibm.com/software/products/en/ibmilogcpleoptistud, last accessed August 2014.

[40] Espiritu, J. F., Coit, D. W., & Prakash, U. (2007). Component criticality importance measures for the power industry. Electric Power Systems Research, 77(5), 407-420.

[41] Pomerol, J. C., & Barba-Romero, S. (2000). Multicriterion decision in management: principles and practice (Vol. 25). Springer.

[42] Al-Sharrah, G. (2010). Ranking using the Copeland score: a comparison with the Hasse diagram. Journal of chemical information and modeling, 50(5), 785-791.

[43] Power system test case archive, available at: http://www.ee.washington.edu/research/pstca/, September, 2014.

[44] Lipowski, A., & Lipowska, D. (2012). Roulette-wheel selection via stochastic acceptance. Physica A: Statistical Mechanics and its Applications, 391(6), 2193-2196.